

User's Guide

Grayteq DLP Management Suite
and Grayteq DLP



User's Guide for Grayteq DLP Management Suite and Grayteq DLP

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Legal Notice

Important Notice!

THE DOCUMENTATION FOR ALL GRAYTEQ SOFTWARE IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SEALAR, INC. SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

Grayteq™, Grayteq, the Grayteq Logo, the Sealar Logo and Safety First are trademarks or registered trademarks of Sealar, Inc. or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This Grayteq product may contain third party software for which Grayteq is required to provide attribution to the third party ("Third Party Programs"). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses.

The product described in this and any similar Grayteq documents are distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this or any similar Grayteq documents may be reproduced in any form by any means without prior written authorization of Sealar, Inc. and its licensors, if any.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Notice.

Copyright © 2012, Sealar Inc. All rights reserved.

Technical Support

Grayteq Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group works collaboratively with the other functional areas within Grayteq to answer your questions in a timely fashion.

Grayteq support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis

For information about Grayteq Support Services, you can visit our Web site at the following URL:

www.grayteq.com/en-us/Support/

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.grayteq.com/en-us/Support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
- Error messages and log files
- Troubleshooting that was performed before contacting Grayteq
- Recent software configuration changes and network changes

Licensing and registration

If your Grayteq product requires registration or a license file, access our technical support web page at the following URL:

www.grayteq.com/en-us/Support/

Customer service

Customer service information is available at the following URL:

www.grayteq.com/en-us/Support/Services/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Advice about Grayteq Technical Support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals

Additional enterprise services

Grayteq offers a comprehensive set of services that allow you to maximize your investment in Grayteq products and to develop your knowledge, expertise, and global insight, which enable you to manage your business risks proactively.

Enterprise services that are available include the following:

- Training
For our valued customers we offer a one and a half day training session. During the session the attendees can learn the theory of the Grayteq DLP software package, and will gain practical knowledge about the usage and maintenance of their Grayteq DLP. After the completion of the training, an educated IT expert will be able to install, operate, and maintain Grayteq DLP.

To access more information about enterprise services, please visit our Web site at the following URL: www.grayteq.com/en-us/Support/Services/

Table of Contents

User's Guide for Grayteq DLP Management Suite 12 and Grayteq DLP 12.....	2
Legal Notice.....	2
Technical Support.....	3
Contacting Technical Support	3
Licensing and registration	4
Customer service.....	4
Additional enterprise services	4
Table of Contents	5
Getting Started	8
What's new in Grayteq DLP 12.....	8
Components of Grayteq DLP Management Suite	11
Architecture.....	12
Installation.....	13
System Requirements.....	13
Pre-installation.....	15
Partitions	15
Test measurements.....	15
Storage sizing.....	15
Ports and protocols	17
Remote Installation requirements	17
Installation	18
Simple installation.....	18
Conventional installation	19
Initial startup	19
Security Server settings	20
Client installation via Security Orchestrator	21
Manual Client Installation	22
Component updates.....	23
Log Filters.....	24
Use SQL for logs	24
SYSLOG.....	25
Security Server fine tuning	25
License handling.....	26
Post Installation	27
Views and Panels.....	27
Save configuration files	27
Uninstall.....	27
Administration.....	29
General	29
Glue, Float, Dock	29
Settings	30

Summary View	32
New view	32
Logs view	32
Monitor	33
Report	33
File Lifecycle Tracking (FLT)	34
Storage Lifecycle Tracking (SLT)	34
Auto Report	34
Alert	35
Policies view	36
Log Filter	36
Event Control	37
Application Policy	38
Snapshot	39
Device Control	40
Storage Control	41
Printer	42
Quarantine	42
Data Vault	43
Policy Group	45
Intrusion Prevention	45
Hosts, Host Groups, Every Host, Host Statistics	46
Users, User Groups, Every User	47
Maintenance view	48
Install	48
License	48
Update	48
Server Log	48
Servers	49
Operators	49
Archives	49
SYSLOG Settings	49
SQL Settings	50
Server Properties	50
Security Server command line switches	52
Support ID	52
Recently updated Support IDs	52
Support IDs	52
Remove Client	61
Manual Remove	61
Remove Client via Security Orchestrator	61
Troubleshooting	62
.....	62
Known compatibility Issues	62

Computer crash.....	62
Remote Installation	63
Failed remote installation	63
Slowdown	64
Security Server slow down	64
Client slow down	64
Security Orchestrator slow down	64
Application Logs	65
Security Server Error Log.....	65
Security Server Status Log	65
Client Error Log	65
Security Orchestrator Error Log	65
Unreasonable local logging	66
Disaster Recovery.....	67
Introduction.....	67
Data.....	67
System datasheet	67
Data to backup.....	67
Disaster types.....	67
Misconfigured Client Policies	68
Damage or destruction of running environment	68
Loss of function.....	69
Error handlings, reporting	70
Glossary.....	71

Getting Started

This chapter includes the following sections:

- [What's new in Grayteq DLP](#)
- [Components of Grayteq DLP Management Suite and Grayteq DLP](#)

What's new in Grayteq DLP

The current release includes the following new features which make Grayteq DLP easier and more efficient to use.

For more information, see Grayteq DLP change log on our web site:

www.grayteq.com/redirect.aspx?URLID=36

Feature	Description
Data Vault	From present version, product versioning and version display changed. In forthcoming editions, the year number will represent major versions, while service pack numbers will represent minor versions. Hotfix versioning remains intact.
Snapshot Protection	Applying screen-on layers on protected information to save from being screenshoted enhanced snapshot protection. Screenshoting is disabled on every screen appearances of protected information, while creating snapshots on unprotected documents, files or information remain uninterfered.
License Stash	In opposition with previous Grayteq DLPs, revoked or unused licenses can now be transferred back to a license stash wherefrom can be re-distributed to new workstations or servers for the remaining license periods.
Client Uninstall	With appropriate Grayteq admin rights, you can now uninstall client from remote. No more on-site client uninstallation is needed. Just simply sit in front of the Security Orchestrator, select Client to remove and click uninstall and Grayteq DLP 12 does the rest.
Application Policy	Games, unauthorized browsers, instant messengers and other unwelcome applications can impact your business with their drain on employee productivity. Social media tools that are meant to aid people staying connected can also be a distraction. Create White-, Gray-, and Blacklists for all applications and decide how applications should operate or even being rejected. Whitelisted applications run smoothly, while unwanted or known harmful applications are denied by Blacklists. For millions of unlisted applications, setup Graylist actions to manage apps from not known sources or with no security clearance.
Whitelist Plus	Application Policy Whitelist Plus is an extra option for releasing quarantine breaching applications in special circumstances. For more information about Application Policy Whitelist Plus please, consult with User's Guide.

Feature	Description
App Policy Test Mode	Do you like the new Application Policy feature, but have no experience in managing applications on this way? Are you worried of applying an app black listing policy in your live environment, but have no test environment to test the given policy properly? No need to hesitate prior to applying and Application Policy in live environments anymore. App Policy Test mode enables to apply policies without any unexpected consequences. Turn test mode on and Grayteq DLP 12 acts like the App Policy would be in force, without de facto denying the application to run and risking system breakdowns or application failures occurred by a failed policy.
Auto Backup	Backup security server configuration and license files. Automatically or Scheduled save for the configuration and license files, to ensure smooth restore in case of any system failures in one move.
On/Off-Network Policy	Data security issues may vary depending on where you are. More protection is available within the office, while strengthened policies are applicable on mobile equipment. On/Off-Network Policy makes security policy management easy to apply within the corporate perimeter and beyond. With Grayteq DLP 12's On/Off-Network Policy, you flexibly can orchestrate various security policies for different locations, situations and circumstances.
Policy Lock	Grayteq DLP 12 locks a policy while being edited by an admin making other admins unable to interact with it. In previous versions an admin could have interfere with another admin's work by attempting to open or modify the same policy in the same time. This interference and its possible consequences are corrected in this version.
Printer Policy	On top of setting up Positive and Negative Log Filter, Event Control for Normal and Removable Media, Application Policy, Snapshot and Quarantine policies, Printer Policy setup were added to right-click policy creation options. Just right-click on a log event and create whatever policy you like by using the log's stored information as presets.
Triggered Alert	Setup which policy breaching attempt may trigger Alert on a new wizard page or simply right-click on a log event and select Alert to create alert if the given conditions are met.
Redesigned Security Orchestrator	On top of visual enhancements and new features integrated, Security Orchestrator's log, policy, report, lifecycle tracking and management display capabilities were radically enhanced. When you need a little more room for your logs, archives, policy wizards or setups, the new Security Orchestrator layout lets you use your display spaces more effectively and quickly navigate among them. Rearrange, add and remove space to or from any displayed element with ease. Moving windows from their original location to floating state is as easy as restoring the original layout. With its redesigned and optimized Security Orchestrator surface, Grayteq DLP 12 enables easy-to-use security policy management, transparent security log views and analysis, while re-organized features make DLP 12 the most handy Grayteq Solution ever.

Feature	Description
Logging Enhanced	Grayteq DLP 12 advances interaction and activity logging to a new level. Monitor, log, report and alert all any user interactions to your valuable corporate data, irrespectively that the given action meets the security policies, or even attempts to breach it. Archive your logs on a forced or on automated way to ensure that not a single log gets damaged or lost.
Report Modifications	Default report type is set to Report and selector got disabled. Only Report type Auto Reports can be created from DLP 12. Auto Report created with previous versions of Grayteq DLP, with the types of Standard FLT From Time, Standard FLT from Time or Creation, Get Existence History, Get Origin, Get Origin and Generate Standard FLT still work in current version.
Detailed Views	Log view is about to receive some great new features. In Log and Report detail views, you can easily learn all necessary information of a given action by just double-clicking on it, and finding out everything you want to know on the summary page. If you're looking for a specific section or detail of a log event, you can now browse in the summary page.
Category View	In Security Orchestrator all new and old features are integrated into category views, enabling faster, more efficient and targeted browsing amongst them. Monitoring, Auditing, Endpoint Protection, Data Protection, Operation Controls and System Fine Tuning categories are easing the navigation and help you to find whatever feature you are looking for.
Forced Archiving	If stored real-time logs consummate more storage space than you want and scheduled archiving is afar? Force interaction log archiving by a single click on the menu bar and clear-up space for interaction logs on the Security Server.
Server Logs	Security Server logs are transferred into Windows event- and security logs, enabling the admins to track specific Grayteq Security Server events directly from Windows logs. These might be server init, error or warning events.
Auto Archiving	Setup archiving schedules to ensure automated log archiving by archive size, number of archived elements or archive timeframe. More regular automated archiving results more protection on all-time logs against being lost, damaged or broken.
Admin Action Logging	Log all policy modifications and changes in a separated log that enables to insight security admins' interactions to policies. Admin action logging logs all Grayteq Admin made modifications, revocation, and application on any security policies.
Database Support	With DLP 12, Oracle 10G and Microsoft SQL 2008 R2 are joining to the list of supported databases, making Oracle or the newest SQL running organizations capable of integrating their Grayteq logs into their existing databases. For helping SME companies in smooth integration, PostgreSQL has also joined the list.
Host ID Priority	In host list, arrange and filter hosts by selecting primary identifier. Primary IDs can be NetBIOS, IP or DNS names. All fields can be switched on or off except the all-time first priority

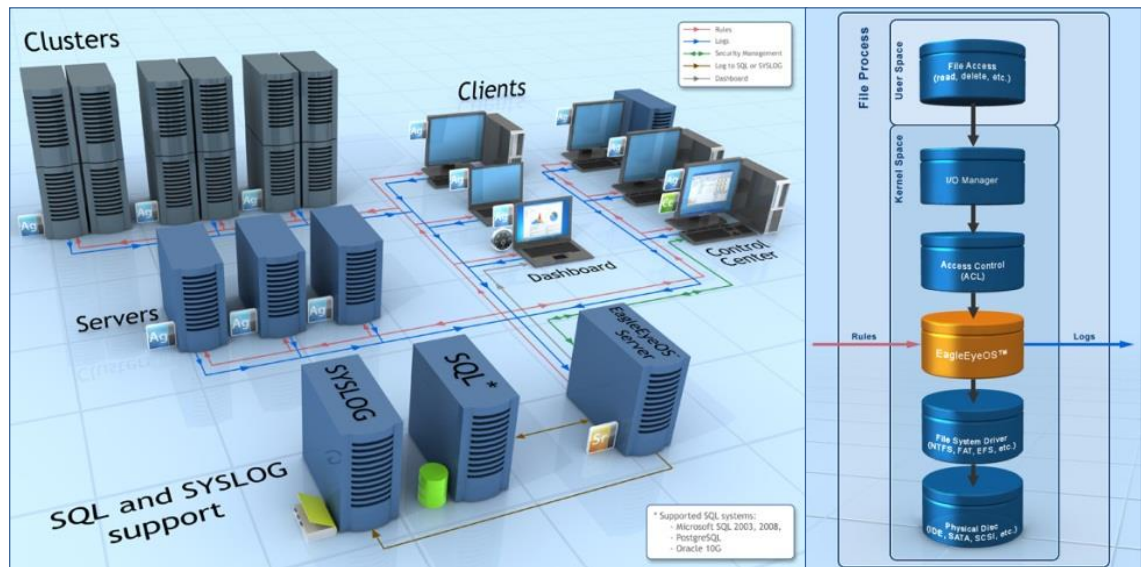
Feature	Description
	one.

Components of Grayteq DLP Management Suite

Grayteq Data Loss Prevention system consists of the following:

Component	Description
Security Server	Security Server is the main component of Grayteq DLP system. Security Server stores security Policies and deploy them to Clients. Gathers and processes incoming logs and provides data to Security Orchestrator and SQL or SYSLOG systems, if in use. Security Server generates Alerts according to preset Alert conditions and enables full control on all Grayteq system components.
Client	Client is the client-side component of Grayteq DLP. Client is embedded within the Operating System kernel, to ensure overall control on operations. It logs events occurred on the client computer, and enforces security policies. If Grayteq Security Server is unavailable (Client is in Off-Network Status), the Client continues logging locally and upholds the enforcement of all preset policies. Client types are the followings: ■ Client with Client CAL: Client for workstations; policy enforcement starts at the operating system boot-up. Logging starts, at user sign-in only; ■ Client with Server CAL: Client for Hosts that operate as Servers; logging and policy enforcement starts at the operating system boot-up; ■ Client with Cluster CAL: Client for Clusters Servers; to protect either active and passive cluster server formations. identically to Server CAL, logging and policy enforcement starts at the operating system boot-up;
Security Orchestrator	Security Orchestrator is the central management interface (GUI) of Grayteq DLP, wherein all activities, policy creation, reporting, alerting, etc. occur.
Dashboard	Newly developed Grayteq Dashboard 12 makes corporate security maintenance easier and more flexible, by extending built-in reporting capabilities of Grayteq DLP 12. Set severity level in various policies to identify and categorize threats.

Architecture



See a standard Grayteq DLP system architecture on the picture above, wherein Grayteq Security Server module runs on a dedicated server, Security Orchestrator and its protecting Client runs on a desktop host, and all other hosts are protected by various Clients. Grayteq Security Server module distributes policies and setting network-wide and Clients enforce them and log all activities. Activity logs are sent to Grayteq Security Server module, wherein various reports and alerts can be generated by Security Orchestrator.

If SQL and/or SYSLOG servers are in use, there is an option to use any of these databases instead of Grayteq's own database for logging, alerting, log storing and analyzing.

Different types of Clients are in use on different types of computers, to distinguish host, server and cluster server groups from each other. It is recommended to install Client with Server CAL on file servers, to log all events even if there is no user logged in. Use Grayteq DLP Client with Cluster CAL, for cluster servers, a special Client type developed for active-passive server clusters. Grayteq policies embed and operate in the operating system core (kernel level operation), amongst OS access right management (ACL) and the file system drivers (FSD).

This adaptation ensures that Grayteq DLP protection cannot be bypassed.

Installation

This chapter includes the following sections:

- [System Requirements](#)
- [Pre-installation](#)
- [Installation](#)
- [Post Installation](#)
- [Uninstall](#)

System Requirements

Grayteq DLP supports both 32- and 64-bit versions of the operating systems listed above.

Grayteq DLP Security Server

Component	Requirement
Operating System	■ Windows Vista ■ Windows 7 ■ Windows 8 ■ Windows Server 2003 ■ Windows Server 2008 and 2008 R2
Hardware	■ Pentium IV 2,6 GHz or a higher performance CPU ■ 512 MB RAM ■ 20 GB free disk space for embedded database ■ NTFS file system ■ TCP/IP based network interface card
Database	Grayteq DLP uses an embedded database, but an external database can be selected optionally. The following external databases are supported: ■ Microsoft SQL Server (up to SQL Server 2008 R2) ■ PostgreSQL Server in unicode mode ■ PostgreSQL Server in ANSI mode ■ Oracle 10G Database Server
Other	Static IP address recommended

Grayteq DLP Client

Component	Requirement
Operating System	■ Windows Vista ■ Windows 7 ■ Windows 8 ■ Windows Server 2003 ■ Windows Server 2008 and 2008 R2

Component	Requirement
Hardware	■ Pentium III 500 MHz or a higher performance CPU ■ 128 MB RAM, ■ 20 MB free disk space and other 2 GB for off-site ■ TCP/IP based network interface card

Grayteq DLP Security Orchestrator

Component	Requirement
Operating System	■ Windows Vista ■ Windows 7 ■ Windows 8 ■ Windows Server 2003 ■ Windows Server 2008 and 2008 R2
Hardware	■ Pentium IV 2,6 GHz or a higher performance CPU ■ 1 GB RAM ■ 50 MB free disk space ■ 1024x768 True Color display ■ TCP/IP based network interface card
Other	■ .NET Framework 2.0 or later ■ Internet connection for license activation is recommended

Grayteq Dashboard

Component	Requirement
Operating System	■ Windows Vista ■ Windows 7 ■ Windows 8 ■ Windows Server 2003 ■ Windows Server 2008 and 2008 R2
Hardware	■ Pentium IV 2,6 GHz or a higher performance CPU ■ 1 GB RAM ■ 50 MB free disk space ■ 1024x768 True Color display ■ TCP/IP based network interface card
Other	■ .NET Framework 4.0 or later ■ Internet connection for Connection CAL creation is recommended

NOTE: All component of Grayteq DLP run well on Windows XP SP3 operating system, but not officially supported.

Pre-installation

Partitions

It is recommended to store Archive and Log Files on separate partitions or on backup storages.

Before installation it is recommended to split the target system into three separate partitions, whereon:

1. Primary partition for the system files
2. Secondary partition for the Security Server log files (active logs)
3. Third partition for archive files

NOTE: In case of using SQL server for log storing, it is recommended to install it to a separated computer.

Test measurements

IMPORTANT: Data published hereunder are valid for general hardware configuration and for informational purposes only. In certain cases, recorded data may vary.

Hardware Configuration			Events entry in the log / second		
CPU	Memory	HDD	10 Clients	100 Clients	350 Clients
1xP Centrino 1,7 GHz	1 GB	SATA 100	7680	6200	6030
1x P4 Xeon 3,06 GHz	2 GB	SCSI UW3	3200	3170	2920
1xP4 3,2 GHz	1,25 GB	SATA 100	3800	3100	2900

Storage sizing

The following formula helps to calculate log file storage consumption (in megabytes) in a monthly period:

$$MByte = \frac{CLNTN * WKH * 25 * (OFFN + ERPN + MDN + OTHN + 20)}{1024^2} * MWD$$

Formula contents

- **CLNTN** - Number of Clients connected to the Grayteq DLP Security Server
- **WKH** - Working hours per day
- **OFFN** - Repartition of Office applications installed on Clients that connected to Grayteq DLP Security Server, in percentage, value to be multiplied by two. Example: in case if every Client use Office application, whereas the no. of Clients is 100, this value is two hundred (200)
- **ERPN** - Repartition of ERP applications installed on Clients, connected to the Grayteq DLP Security Server, in percentage, value to be divided by two. Example: in case if every Client use ERP applications, whereas the no. of Clients is 100, this value is fifty (50)
- **MDN** - Repartition of the media usage on the Clients, connected to the Grayteq DLP Security Server, in percentage, value to be divided by two. Example: in case if every Client use media files, whereas the no. of Clients is 100, this value is fifty (50)

- **OTHN** - Repartition of other, important applications connected to the Grayteq DLP Security Server, in percentage, multiplied by the number of monitored applications. Example: in case of two specially monitored applications had been installed on every Client, whereas the no. of Clients is 100, this value is two hundred (200)
- **MWD** - Working days per month

Calculation formula for Snapshot storage consumption

By creating a Snapshot, Grayteq DLP Security Server uses approximately 80 KBytes of disk space. The following formula helps to calculate Snapshot storage consumption (in megabytes) in a monthly period:

$$MByte = \frac{80 * \left(\frac{CLNTN + USRN}{2} \right) * SNRL * NDEV * MWD}{1024} / SLVL$$

Formula contents

- **CLNTN** - Number of connected Clients to Grayteq DLP Security Server.
- **USRN** - Number of Users of monitored resources.
- **SNRL** - Number of Snapshot Policies.
- **NDEV** - Number of Snapshot Policy violations per day per user.
- **MWD** - Working days per month
- **SLVL** - Snapshotting frequency in seconds
 - High level security: **1**
 - Elevated level security: **2**
 - Normal status: **5**
 - Good performance: **10**
 - Best performance: **15**

Example

A company runs 100 computers; with significant Microsoft Office component usage. Five of IT department recently listen digital audio files and use special network management software. The company works 20 days a month, 8 hours a day. Ten Snapshot Policies are set and snapshots created 5 times a day per user, average. Snapshotting frequency is set to Normal status. Parameters detailed above are as follows:

Name	Value
CLNTN	100
WKH	8
OFFN	200
ERPN	0
MDN	2,5
OTHN	5
?WD	20
USRN	100

Name	Value
SNRL	10
NDEV	5
SLVL	5
Log Files total (MByte):	86,78/Month
Snapshot storage size required (MByte):	2.343,75/Month

Ports and protocols

Default Grayteq DLP Security Server communication protocol and port is: **TCP/3999**

NOTE: Grayteq Security Server does not initiate Grayteq specific communications. Clients and Security Orchestrators initiate Grayteq related communications to the Security Servers only. Accordingly, limiting data connection initializations' direction can ensure Grayteq Security Servers' border protection.

Grayteq DLP Security Server initiates administrative communication on the following ports/protocols:

- DNS name service requests to default DNS server port: **UDP/53**
- Workgroups, Active Directory access: **UDP/445**
- Remote installation; over Microsoft File Sharing protocols: **UDP/139, TCP/135, UDP/445**
- Microsoft SQL log transmission to SQL server: **TCP/1433**
- PostgreSQL log transmission to SQL server: **TCP/1395**
- Oracle SQL log transmission to Oracle server: **TCP/4321**
- SYSLOG logging to SYSLOG server: **UDP/514**

Remote Installation requirements

Pre-requisites for remote installation of the Grayteq DLP Client:

- Grayteq DLP Security Server must operate in the name of a user with full access rights on system folders and files of the targeted host. It's the easiest to achieve it with Domain Administrator right. If the Grayteq Security Server runs by the Grayteq Security Server System Service, then the service running user must meet the access right criteria detailed above.
- Load the Security Server version matching Client Installer file (*.gup) into the Security Orchestrator.
- The designated host shall be the member of the domain, which domain's administrator rights are in use for running the Security Server.
- Enable Administrative Shares on the host. Minimum admin share requirements: IPC\$, ADMIN\$ and the administrative sharing of the system drive (the drive where Windows is installed), (for example: C\$).
- If the designated host runs firewall, then enable "Microsoft File and Printer Sharing" services from the local intranet.
- Grayteq Admin that logged into Security Orchestrator must have rights for section Maintenance, Administrators.

Installation

1. Run Grayteq DLP Security Server first. Install Grayteq Security Server System Service - the service in charge for continuous run of the Security Server - beside the Security Server.
2. Install Security Orchestrator to a host that will be in use as administrative center of the system. First two steps of installation can be merged if Security Server and Security Orchestrator are running on the same host.
3. Security Server may remotely install Clients, upon installation command of the Security Orchestrator.

Installation methods:

- Simple installation
- Conventional installation

WARNING: Setup test environment separated from your corporate live system, to avoid any system malfunctions or unexpected results. **Installation to corporate live systems is EXPRESSLY NOT RECOMMENDED prior to test environment experiences!**

Simple installation

Security Server and Security Orchestrator are installed into %ProgramFiles%\Grayteq\DLP folder, by default.

Clients can be installed on the following ways:

- Remote installation by Security Orchestrator
- Local installation at hosts

Installation steps

1. **Select setup language**, then click **Ok**

NOTE: Setup language selection affects the installation procedure, system tray and start menu, only. Security Orchestrator language settings can be set later, irrespectively to this setting.

2. **Check, if the newest software version** is to install on Welcome screen, then click **Next**,
3. **Read the** End-User License Agreement (EULA) thoroughly and **Accept** it if you agree, then click **Next**,
4. **Choose Installation method** and click **Next**
5. **Set Grayteq DLP shortcut appearance** on Desktop, then click **Next**
5. Installation starts here
6. Click **Finish** to complete installation

Conventional installation

At conventional installation, you can select the components to install. This installation mode allows to skip Log Filter and Client installation packages' installation.

Installation steps

1. **Select setup language** and click **Ok**

NOTE: Setup language selection affects installation process, system tray and start menu, only. Grayteq DLP's language settings can be changed later, irrespectively to this setting.
2. **Check, if the newest software version** is to install on Welcome screen, then click **Next**,
3. **Read the End-User License Agreement** (EULA) thoroughly and **Accept it** if you agree, then click **Next**,
4. **Choose Installation method** and click **Next**. Select Components to install and click **Next**
6. Select Start Menu Folder
 1. Program will be installed into %ProgramFiles%\Grayteq\DLP folder by default
 2. If you want to install to another folder, click **Browse**, **Select target folder** and click **Next**
7. **Set Grayteq DLP shortcut appearance** on Desktop, then click **Next**
8. Installation starts here
9. Click Finish to complete installation

Initial startup

Security Server startup

Start Menu >> All Programs >> Grayteq >> Grayteq DLP >> Security Server >> Grayteq DLP Security Server

Grayteq Security Server console window appears at successful startup.

Appropriate Security Server startup

Upon receiving the following messages, you can be sure that Grayteq Security Server is up and running.

NOTE: Successful Security Server startup messages are the following:

- I- DISPATCHER: Starting network communication
 - I- Host Watcher Thread started
-

Inappropriate Security Server startup

Upon receiving any message starts with an **-E-** (an error code), Security Server startup failed.

NOTE: For help please, ask Grayteq Support by sending an e-mail with proper error description and the **-E-** code to support@grayteq.com

Security Orchestrator startup

Start Menu >> All Programs >> Grayteq >> Grayteq DLP >> Security Orchestrator >> Grayteq DLP Security Orchestrator

Note: To login to Security Orchestrator at first time, use the default Operator, named **John**, and his password is **Doe**.

Server settings

Create new Operator

1. Go to **Maintenance** view
2. Click **Operators**
3. Default Operator is John. **Double-click** on name John
4. **Set Screen name and e-mail address** for the New Operator, and click **Next**
5. **Set Password**, and click **Next**
6. **Set New Operator's rights.**

NOTE: For smooth operation, set super-user rights to the New Operator by **Selecting All**, and click **Next**

7. **Set Operator login name**, and click **Next**
8. Click **Save**, to finish

WARNINGS: Operator and Password fields are case-sensitive!

Login with New Operator

1. Press **Ctrl + L** or select Server to login, in File menu, Connection submenu.
2. In pop-up window, **reset Operator name John to new Operator name** and **enter new Operator password**, then click **Login**

NOTE: Current Operator name appears with bold letters.

Modify Security Server folders

By default, Grayteq DLP Security Server creates the following folders in %ProgramFiles%\Grayteq\DLP\Server folder:

- **Archives:** to store Archive Files
- **Auto Report:** for the results of Auto Reports and Alerts
- **Backup:** for secure system backups
- **Error Report:** for application errors
- **Log:** for current Log Files
- **Report:** for information needed to Auto Reports and Alerts
- **Statistics:** for database files for Grayteq Dashboard 12 support.
- **Update:** for Installation Files loaded into Security Orchestrator

NOTE: Error Report folder is generated automatically even, if there is no error in Security Server application.

NOTE: Archives folder is generated upon first archivation only. Log archivation presets: after 30 days of operation or if log size exceeds 47 MB.

Separate Archives

Perform the followings to store Logs/Archives and Secure Backups separately:

- Make sure that Grayteq DLP Security Server is stopped
- Start Command Prompt
- Go to Server folder %Program Files%\Grayteq\DLP\Server\

- Start Security Server with the following command: **GrSrApp.exe /reconfigurepath**
- Upon proper authentication, storing locations of Logs, Archives and/or Secure Backups can be set by **/reconfigurepath** command, in drive:\folder structure.
- **Security Server auto-stops** at this point

IMPORTANT: New folder names must end with “\” sign.

Client installation via Security Orchestrator

Pre-requisites for Grayteq DLP Clients remote installation

- Run Grayteq DLP Security Server application on behalf of a user with full system authorities (best practice: Domain Administrator rights user). If Security Server application is operated by the Grayteq Security Server System Service, then this service’s executing user must have the authorities mentioned above.
- Load Security Server application version matching Client installation file (*.gup) into Grayteq DLP Security Orchestrator
- Target computers and the Server shall be members of the same Domain.
- Enable Admin shares on target hosts. IPC\$, ADMIN\$, and System Drive admin shares are required.
- Enable “Microsoft File and Printer Sharing” service on target computers’ firewall.
- Security Orchestrator Operator must have rights for Maintenance and Operators sections.

Remote installation steps:

1. Insert Installation Package into Grayteq DLP Security Server
 1. Go to **Maintenance** view in left hand side Navigation panel, and select **Update**
 2. Set **Source** to „**From File**“, then click **Open**
 3. Browse Installation Package that is in %ProgramFiles%\Grayteq\DLP\Installers folder by default.
 4. Select update file with **.gup extension**
 5. Message notifies you about successful Installation Package insert.
2. Remote installation via Security Orchestrator
 1. Go to **Maintenance** view in left hand side Navigation panel, and select **Install**
 2. Select network **Source** from the following:
 - **Network:** Browse network for currently present computers.
 - **Active Directory:** List of computers in Active Directory
 - **Novell Network:** List of computers in Novell Network
 - **Specific Host:** Select specific host
 3. Select computers, to install Clients
 4. In Settings menu, select **Installation Package Version** to install, and click **Install**
 5. Server Log notifies you about successful installation, or click **Show Install Log** for detailed installation information.

Installation results may:

- **Finished:** Installation finished successfully and Grayteq DLP Clients are in use
- **In Progress:** Installation is in progress

- **No End-Point:** Requested Host is off, or unreachable
- **Access Denied:** Requested Host is off, or doesn't meet installation pre-requisites
- Installation Failed: **Installation failed, due to an unrecoverable error**

Manual Client Installation

There are certain cases, when installation cannot be executed through the Security Server. Such a case is when Grayteq DLP Security Server cannot run with elevated access rights that are necessary for the remote installation. In such cases, manual installation or remote installation service (like SCCM), might install Clients.

Pre-requisites for manual installation:

- Local admin rights for the installation and initial Client setup.
- Exact DNS name or IP address of the Grayteq DLP Security Server running host.

Double-click on installer or use command prompt for installation. The following parameters are in use at command prompt installation:

- `/verysilent`
By using this parameter, the install wizard does not appear, while the installation occurs in the background, fully hidden from the user.
- `/norestart`
Use of `/verysilent` parameter might cause that the designated host is to be restarted at the end of installation process. By using this parameter, automated restart can be avoided.

WARNING: In opposition to the Security Server assisted Client installation, the Client does not auto run at the end of installation, because it's not known to which Grayteq DLP Security Server the Client has to connect.

First setup steps of manually installed Client:

1. Run Command Prompt by executing **cmd.exe** with elevated rights. No matter if you have Local Admin rights on the given workstation, still use Run as Administrator right-click option.
2. Browse into the folder of the installed Client:

```
cd "\\Program Files\Grayteq\DLP\Client\"
```
3. Execute the Security Server setup command:

```
grclsvc.exe setserver <Security Server domain name or IP address >
```
4. Run Grayteq DLP Client

```
grclsvc.exe start
```

Component updates

Security Orchestrator update

Stop Security Orchestrator, and then run installation application to update.

Security Server update

WARNING: To avoid Log file damage, you have to perform proper Security Server shutdown via Security Orchestrator.

1. Go to **Maintenance** view
2. Select **Servers** on Navigation panel
3. Select **Server** in use
4. Click **Stop** button, to stop Server in use
5. **Run** Security Server installation package

Client update

1. Switch to Maintenance view, then click on Update option
2. Insert **new Client installation package** into Security Server
3. Select **Hosts** to update
4. Select **software version** to install
5. Click Update button, then enter **update description**
6. Click **Update** button on pop-up menu to start Client upgrade.

If Internet access is not available, system warns you in a message. Click on **Connection Settings** menu to set necessary information for accessing the Internet. Upon proper authentication, you can download Updates, by entering your user name and password you used during registration on <http://www.grayteq.com/en-us/Support/> website.

WARNING: Backup your Grayteq DLP system, prior to update or upgrade!

WARNING: Revise Operator authorities after successful update, because new Operator rights WILL NOT be automatically added to existing ones.

Log Filters

Grayteq DLP logs every event occur system-wide meaning that all system and file events will be logged, to avoid information loss. Log Filters enable to filter any security-irrelevant events to being logged. These events can be temporary internal processes of applications, system events and any other events you consider security-irrelevant.

WARNING: Careful circumspection at Log Filter creation is vital, when improperly set Log Filters may deprive you from valuable log information.

Default Log Filter Package (log-filters-pack.gfe) is installed into %ProgramFiles%\Grayteq\DLP\SO\Exports path. Import Log Filter package, by using Import button in Policies view. Create your system-specific Log Filters to optimize the amount of logs and set proper logging policy for your system specialties. Assign every newly developed log Filters to Every Host.

Assign Log Filter

For easier navigation choose the dual-window view

1. Go to **Policies** view, select **Remote Items** and then **Log Filter**
2. In the other window, select **Host**
3. **Drag and Drop** selected Log Filter on Host of Host Group

Add a Policy to a Policy Group, by applying the same drag and drop method as detailed above, accordingly.

Use SQL for logs

Supported databases

- Microsoft SQL Server
- PostgreSQL Server in unicode mode
- PostgreSQL Server in ANSI mode
- Oracle Database Server

TIP: Grayteq DLP Security Server checks every connection for database or table structures of SQL Server. Missing database elements get automatically created, based on the default configuration of SQL Server. If default configurations are not appropriate, create new database that meet your needs, under Grayteq name.

Find more information for Microsoft SQL Server installation on the following page:
[http://msdn2.microsoft.com/en-us/library/aa197926\(SQL.80\).aspx](http://msdn2.microsoft.com/en-us/library/aa197926(SQL.80).aspx)

SQL Settings

1. Open **Security Orchestrator**
2. Go to **Maintenance** view
3. Click **SQL**, then Enable **SQL** server
4. Set the necessary **user name** and **password**, or choose **Use Windows Authentication**, and select connection **Protocol**
5. Select **Database Type**
6. Enter **Database-** and **Datatable names**. Leave these field blank to use the following default settings:

Database Name: Grayteq

Table name for Log elements: event_logs

Table name for Snapshot images: event_pictures

7. Click **Save**
8. Restart Grayteq DLP Security Server

WARNING: By turning SQL Server on, Grayteq DLP License validation policy changes. In this case, events will be logged from Hosts with valid licenses only. Using SQL, there is no possibility to restore log files from Hosts without valid licenses.

SYSLOG

Supported SYSLOG systems - without the need of completeness: HP OpenView, IBM Tivoli, Cisco MARS, Novell Nsure Audit

To turn on SYSLOG, follow the next steps:

1. Open **Security Orchestrator**
2. Go to **Maintenance** view, click **SYSLOG** icon and enable
3. Set SYSLOG server **connection parameters**, and **general name** to appear in SYSLOG log
4. Set **Messages** to transfer to SYSLOG from the following, then click **Next**:
 - Auth Success, Error, Info, Warning
5. Set **Auto Reports** and **Alerts** to register in SYSLOG, and click **Next**
6. Set **Events** to register in SYSLOG from the following, then click **Next**:
 - Create, Overwrite, Read, Open, Modify, Copy, Move, Delete, Run, Process End, Copy and Paste
 - Print, Encrypt, Decrypt, Storage Connect, Storage Disconnect, System, Copy Destination,
 - Copy Source, Folder, Move Destination, Move Source
7. Set **Results** to register in SYSLOG from the following, then click **Next**:
 - OK, Blocked, No License, Client On, Client Off
8. Click **Save**

Security Server fine tuning

Cascade Spool

Cascade Spool is a dynamic storage wherein the Install and Update Packages of Grayteq DLP Clients and the results of Auto Reports and Alerts are stored.

Auto Reports and Alerts

Grayteq DLP lets you run Auto Reports and Alerts. For rapid access, these data are stored in temporary storage called Cascade Spool. Data are stored in Cascade Spool until preset storage is not full, then the oldest data get erased the first.

TIP: In case of recent usage of these two functions, resize Cascade Spool to at least double size to the original.

Update Packages

Grayteq DLP enables you to remotely mass install Clients network-wide. For rapid access, these data are stored in temporary storage called Cascade Spool. Data are stored in Cascade Spool until preset storage is not full, then the oldest data get erased the first. Modify Cascade Spool reservation for Update Packages on on-demand base only.

1. Open **Security Orchestrator**

2. Go to **Maintenance** view, click **Servers** icon
3. Select **Server**, whereon these settings are to be applied
4. Set values, in **Server Wizard**

Set Snapshotting frequency

Grayteq DLP determines Snapshotting frequency, based on security level setting or available performance. Snapshotting frequency may affect performance of Grayteq DLP Security Servers and Clients in certain cases.

Go to **Maintenance** View, then click **Server properties** wizard, and then click **Performance settings**

- **Snapshot frequency:** Set Snapshotting frequency here. Higher security settings may cause lower performance.

WARNING: Setting Snapshotting frequency to "High security", large amount of Snapshots may be taken, causing significant Log File size enlargement and additional loading on Clients.

Snapshot creating frequency

Minimum period measured in seconds between taking two Snapshots:

- Best Performance: **15**
- High Performance: **10**
- Normal: **5**
- Elevated Security: **2**
- High Security: **1**

Archive setup

In Grayteq DLP Security Server you can set two values for archiving; where there is a logical 'OR' relation between these two values.

- The first value is the number of days, as per default: **30 days**
- The second value is log file size, as per default: **47 MBytes**

According to default settings, when log file reaches the 30th day OR the size of 47 MBytes size, Security Server automatically creates an archive file.

TIP: It is recommended to set Grayteq DLP Security Server to create archive files by 350 MBytes.

License handling

Load License File

Open Grayteq License Manager by clicking on Insert License button.

You can read more here about the [Grayteq License Manager](#)

NOTE: To apply downloaded and activated licenses, assign them to installed Clients.

Assign Licenses to Clients

1. Run **Security Orchestrator**
2. Click **Maintenance** view, then on **License** icon
3. Select **Host** or **Hosts** with no license assigned, where you want to assign licenses.
4. Select **License Type** and click **Activate**.

COMMENT: No license can be assigned to an already licensed host, so be careful with license assignments.

License renewal

1. Go to **Maintenance** view
2. Click **License** icon
3. Select **Host**, whereon you would like to renew the License
4. Click **Insert License**, then download new license with **Grayteq License Manager**
5. In Licenses drop-down menu **select Client type** to renew, and click **Renew**

License transfer

1. Go to **Maintenance** view
2. Click **License**, then set **Client**
3. Select Target Host from **Transfer** drop-down menu
4. Click **Transfer**

WARNING: After license get transferred from a Host, it's not possible to re-assign license to the same host and to connect to Security Server from that Host, anymore.

WARNING: It is possible to transfer a license to a Host with license assigned, but in this case, previously assigned license of the target Host will be lost.

Post Installation

Views and Panels

System customization can be performed via Security Orchestrator. Present chapter introduces the usage of Views and Panels of the Security Orchestrator.

Save configuration files

Grayteq DLP Security Server module running computer, save

- GrSrCfg.dat
- GrSrLic.dat
- SysConfig.dat

Files that can be found in **%ProgramFiles%\Grayteq\DLP\Server** folder.

IMPORTANT: GrSrCfg.dat file contains all configuration information of the newly installed Grayteq DLP system, while SysConfig.dat contains Storage related data.

WARNING: Regular backup of Grayteq DLP Security Server configuration files is very important. System restore from an up-to-date configuration backup is one-click-easy and efficient.

Uninstall

1. Start Grayteq Security Server.
2. Start Grayteq Security Orchestrator and login.
3. Navigate to Policies view, and select Remote Items | Hosts in split window.
4. Browse Host with Client and in its properties (Right-Click menu) turn Client off.
5. Navigate to Maintenance view, and click Servers button.
6. Stop running Grayteq Security Server.
7. Go to Control Panel >> Add or Remove Programs, and uninstall Grayteq DLP.
8. Restart computer.

WARNING: Grayteq DLP can be uninstalled only, if all components are stopped.

Administration

This chapter includes the following sections:

- [General](#)
- [Summary view](#)
- [New view](#)
- [Logs view](#)
- [Policies view](#)
- [Maintenance view](#)
- [Server command line switches](#)
- [Support ID](#)
- [Remove Client](#)

General

You can find some general information in this section.

Glue, Float, Dock

Views

- Full Screen

By selecting Full Screen, Menu Bar and Taskbar are not displayed.

NOTE: Press F11 to switch back to previous view!

- Floating window

By selecting Floating Window, opened file will be displayed in a separated window.

Policies View, selecting Float, will display Items in a separated window, called Policy Displayer that can be Glued, Docked or switched back to Normal view.

By double-clicking on the header of a Floating Window, windows switches to full size, and upon another double-clicking, restores to original view.

- Normal view

Reset floated elements into default view.

Snapshot window

Should you made a Snapshot for the Log file, a Snapshot icon appears in the specific Log line.

- Open a separated window for Snapshot by double clicking on the Report
- Snapshot views can be set in Menu also

Snapshot visual settings:

- **Zoom in 10%** - Zoom picture in in 10% steps. Window center is the center of magnification
- **Original Size** - Resize to original size
- **Zoom out in 10%** - Zoom picture out in 10% steps. Center of the window is the center of zoom out
- **Fit to window** - Fit Snapshot size to window

- **Zoom in** – Zoom Snapshot in in 10% steps. Click on, to define magnification center
- **Zoom out** - Zoom Snapshot out in 10% steps. Click on, to define zoom-out center
- **Zoom Percent** - Set Zooming rate
- Right-click on Snapshot icon to save, copy or send the given Snapshot

Settings

Tools >> Options >> Settings - Ctrl+K

General

- **At Launch**

Here you can select active tab page after log in. Here you can set off-line mode (as default) of the Security Orchestrator. In this case Login window will not appear when starting the Security Orchestrator. You can open selected Server window from the Menu Bar >> File >> Connect to the Server.
- **Language**

Select Security Orchestrator language:

 - Hungarian
 - English
 - Japanese
 - Spanish
- **Other**

You can set here:

 - To turn Use Visual Enhancement on or off (e.g.: message window to set translucent)

TIP: Turn Visual effects off for better performance, if you use a computer with limited resources.

 - To turn Use Sounds on or off
- **Software updates**

Here you can set that Security Orchestrator check software updates for your Grayteq DLP system on the internet every time, when it starts.

Internet connection

- Registration on www.grayteq.com/en-us/Support page
To download Updates type User Name and Password accordingly. These are mandatory fields.
- Proxy Settings
 1. Check in **Use Proxy**
 2. Type **Name** and **IP address** of the Proxy Server
 3. Type connection **Port** of the Proxy Server
 4. Check in **Authentication**
 5. Type **User Name**
 6. Type **User's Password**
 7. Check in **Domain**
 8. Type **Domain Name**

Notifications

Select Events you require Notifications about:

- Logs
 - Report Finished, No Result Report
- Create Policy
 - All, Log Filter, Event Control, Application Policy, Snapshot, Device, Storage, Printer, Quarantine, Data Vault, Policy Group, Intrusion Prevention
 - Unavailable Feature Warnings
- Delete Policy
 - All, Log Filter, Event Control, Application Policy, Snapshot, Device, Storage, Printer, Quarantine, Data Vault, Policy Group, Intrusion Prevention
- Licenses
 - Transfer Success, Insert Success, License Renew Success, Upload Success, No License Available
- Rights
 - Authentication Failed

Wizard

- On Wizard Launch
Click to show Welcome window of the Wizard.
- In Wizard Process
Set to show Properties Panel automatically.
- On Wizard Finish
Set save settings of the Wizard.

Summary View

In this view, you can find a compact summary about your Grayteq DLP System.

Statistical information:

- Computer Summary
Information about your Grayteq DLP protected hosts that run out-of-date versions or even license expired.
- Incident Summary
Summary of your security policy breaches in total and in details per types.
- License Summary
Summary of the licenses of the given Server detailed by level, type, amount, expiration, status and version.
- Server Summary
View your Server statistics right beside your SQL or SYSLOG settings.

TIPP: For more detailed information please, use Grayteq Dashboard Management insight Tool, part of Grayteq DLP Management Suite.

New view

In this view, you can create any type of element that is available in the Grayteq DLP system. Short summary of the given element can be found on the bottom of this view.

Logs view

See Local and Remote Items on Navigation panel.

Accessible functions by Logs view

- [Monitor](#)
- [Report](#)
- [File Lifecycle Tracking \(FLT\)](#)
- [Storage Lifecycle Tracking \(SLT\)](#)
- [Auto Report](#)
- [Alert](#)

Logs view functions

- See Log Items by types
- Reports marked with bold letters. Report name refers to the description, indicating the number of items and, blocked events and its last run.
- Run, stop or delete Reports by Function buttons as follows
 - **Run selected Log Items** - Show the content of selected Log items in reading pane
 - **Update all Log Items** - Update of all Log Items loaded into the selected folder
 - **Stop Report running** - Results of the selected Log Item can be deleted
 - **Report delete** - Delete selected Log Items
 - **Edit** – Modify Log Item properties by Log Item Wizard pops-up

Monitor

Real-time Monitoring: Designed for monitoring and real-time displaying all file interactions occur network-wide. It's significance raises in providing maintenance services on a required level (like immediate follow-up for policy modifications) and in discovering real-time incidents.

Create new Monitor step-by-step

1. Select Events to monitor, select all events to monitor by **Select All** button, or invert your selection by **Invert** button and click **Next**
2. Select Event results to monitor, select all event results to monitor by **Select All** button, or invert your selection by **Invert** button and click **Next**
3. Select Users to monitor, by entering users manually, or browse AD for users, then add by clicking **Insert**

NOTE: If no user is selected, ALL USERS will be monitored.

Manage User list by Add Remote, Insert or Delete All buttons, and click **Next**

4. Set Paths to monitor, by entering paths manually, or browse, then add by clicking **Insert**
Manage Paths list by Add Local, Add Remote, Insert or Delete All buttons, and click **Next**
5. Select Target Paths to monitor

NOTE: This step appears only, if you select Copy and/or Move Events in Select Events step.

6. Set Target Paths to monitor, by entering target paths manually, or browse, then add by clicking **Insert**
Manage Target Paths list by Add Local, Add Remote, Insert, Delete All buttons, and click **Next**
7. Select Processes to monitor, by entering processes manually, or browse, then add by clicking **Insert**
Manage Processes list by Add Local, Add Remote, Insert, Delete All buttons, and click **Next**
8. Select Host to monitor, and click **Next**
9. Set Monitor name and description, saving location (local or remote), set reports to save automatically or view query after save, then click **Save**

Report

Reports query and analyze user events. Should you prepare reports; any kind of stored information can be searched, grouped and ranged in order to find them as fast as possible. Beyond file operations, also special information can be attained e.g.: leaving the protected network, enters, Copy and Paste, etc.

Create new Report step-by-step

1. Select **Events** you wish to get a Report about
2. Select **Result** by Events you wish to create a Report from
3. Set **Users** to show in the Report. If no Users set, Select all will be applied
4. Set the **Path** of the folders you wish to create a Report
5. Set Target Path you wish to create a Report, this step applicable by the Copy, Move events only
6. Set **Processes** you wish to create a Report about
7. Select which **Host** you wish to get a Report from
8. Type the name of the Report you created

File Lifecycle Tracking (FLT)

"Who did what and when with the file? Where and under what name can the file be found?" The File Lifecycle Tracking (FLT) is a specially developed feature to trace what modifications, changes made in a file since its creation. The File Lifecycle Tracking function marks the parallel life-tracks of the file with branches; it is also feasible to search the file's Lifecycle directly from the queried Reports.

Create New FLT

You can create a new File Lifecycle Tracking with right-click option on any log event. This provides correct timing parameters about the given file event for the query.

Storage Lifecycle Tracking (SLT)

It shows if hosts were connected with a specific storage independently from the type of the storage (e.g. pen-drive, photo camera, etc.). The software is able to identify the hardware connected, and displays who, when and on which host the connection was made, moreover what kinds of file operations were executed.

Create New SLT – Storage activity

You can create a new Storage Lifecycle Tracking with right-click option on any Storage related log event. This provides correct timing parameters about the given Storage for the query.

Create SLT – File activity

You can create a new File Activity report any previously queried SLT report with a right-click option on any Storage existence log row. This provides correct timing parameters about the given Storage for the query.

Auto Report

Auto Report enables you to create any form of report or lifecycle tracking and to regularly analyze any activities.

Create new Auto Report step-by-step

1. **Select type** of Auto Report
2. **Set timing** of Auto Report
3. Select Events you wish to get an Auto Report about. This step accessible when you'd like to create Report type based Auto Report.
4. Select which type of Results you want to get an Auto Report by Events. This step accessible when you'd like to create Report type based Auto Report.
5. Select users, you wish to get Auto Reports by its file operations from. If you select none, it applies to all. This step accessible when you'd like to create Report type based Auto Report.
6. Set the Path of folders you wish to create an Auto Report about
7. Select which Processes you wish to get an Auto Report about
8. Select here, from which Hosts you wish to get an Auto Report about
9. Set the time of Log, queried by the Auto Report
10. Set your Auto Report's additional settings
 1. Set if its creator can access Auto Report only.
 2. If **Email** option is selected, set the parameters of the mail server.
 3. Select **intended recipients** from the list of Grayteq Administrators
 4. If you want Auto Report to be erased after its run, you can select it here.
11. Type the name of the Auto Report you created

Alert

Alerts notification is an optional event and gets generated at the moment an event occurred. Alerts can be queried in both Report and File Lifecycle formats. It has great significance at immediate detection of abuses, since it notifies about the root cause of any blocking simultaneously.

NOTE: It's possible to set Alert at certain types of denying Policies. These policies appear under "Policy Violation triggered Alert".

Create new Alert step-by-step

1. Select Events that can trigger the Alert
2. Select what Event Results should initiate Alert
3. Select users, whose file operations you wish to get an Alert of; if you select none, it applies to all
4. Select the Path of folders, which ones' related and selected events should trigger the Alert
5. Select Processes which from you wish to trigger the Alert
6. Select the Host you wish to receive a Report about
7. Select Alert type
8. Select what parameters of the report are to be copied from the alert triggering activity. Later, you don't have to set these parameters again.
9. At Report type Alert, you have to set the following parameters on top of the previous:
 1. Set what Events are to be listed in the Alert. This step is only available at Report type Auto Report.
 2. Set what Results are to be listed in the Report. This step is only available at Report type Auto Report.
10. Set Log times in Alert-generated Report
11. Set after-processes for the Alert
 1. Set if the Alert is available for its creator only
 2. If Email option is selected, set mail server parameters
 3. Select which Grayteq Admins receive Alert-generated Logs
 4. Set if you want the Alert being erased after its run
12. Set Alert name

Policies view

Here you can handle Policies, Hosts and Users that present within Grayteq DLP Management Suite. You can see Hosts' Statistics and dependencies of different items on **Navigation panel**.

Accessible functions by Policies view:

- [Log Filter](#)
- [Event Control](#)
- [Removable Media Control](#)
- [Application Policy](#)
- [Snapshot](#)
- [Device Control](#)
- [Storage Control](#)
- [Printer](#)
- [Quarantine](#)
- [Data Vault](#)
- [Policy Group](#)
- [Intrusion Prevention](#)
- [Hosts, Host Groups, Every Host and Host Statistics](#)
- [Users, User Groups Every User](#)

Log Filter

With the help of Log Filter, events that are irrelevant, don't connected to user activities, have no merit information, and can be filtered. These events can be the temporary internal processes of applications. Network traffic and the entries on Server. By appropriate settings, the size of logs can be decreased significantly.

Creating new Log Filter

1. Select Events that should be filtered by the Log Filter. If there are no selected Events, it will be applied to all.
2. Select the Path of folders which should be filtered by the Log Filter
3. Select Process should be filtered by Log Filter
4. Set Log Filter's options
 - Set the type of the Log Filter:
 - **Positive Log Filter:** it will log preset only
 - **Negative Log Filter:** it will log everything, except the settings
 - Set Policy's **scope**
 - **On/Off-Net:** Policy takes effect irrespectively to the connection status between the Client and the Grayteq Security Server
 - **On-Net:** Policy takes effect until there is live connection between the Client and the Grayteq Security Server
 - **Off-Net:** Policy takes effect until there is NO live connection between the Client and the Grayteq Security Server
5. Set if you want to use time interval, if yes, you can set the date and time
6. Set the name of the Log Filter

NOTE: You have to assign new Log Filter to an object for being applied!

Event Control

Event Controls are those kind of policies which enforce the security of files that when, where, who and with what (what kind of application) can access them.

Creating new Event Control step-by-step

1. Select Events which should be control by the Event Control; if there are no selected Events, it will be applied to all
2. Set Users to be blocked! If you not select any, it will apply to all.

TIP: By checking certain Users, these Users can be set to Exception Users. In this case all Events depicted within the present Policy, will be applied on all Users excluding the Exception ones.

WARNING: If unidentifiable User or Users are set, then these Users are going to be excluded during the inspection of the Policy.

3. Select Paths to be blocked

TIP: By checking certain Paths, these Paths can be set to Exception Paths. In this case all Events depicted within the present Policy, will be applied on all Paths excluding the Exception ones.

WARNING: If Exception Path(s) is set only, then blocking will be applied on all other (non-Exception) Path(s).

4. Set Target Paths to deny and its handling mode. This setting appears if any of the Copy or Move events were selected at the first wizard step.

Target Path handling setup options

- **Exception:** Copy or Move is enabled for the Paths set only
- **Standard:** Copy or Move is Denied for the Paths set only

5. Select Processes to be blocked

TIP: By checking certain Processes, these Processes can be set to Exception Processes. In this case all Events depicted within the present Policy, will be applied on all Processes excluding the Exception ones.

WARNING: If Exception Process (es) is set only, then blocking will be applied on all other (non-Exception) Process (es).

6. More Options

1. Set Event Control type

- **Normal Event Control:** It is to be applied on the complete IT infrastructure without limitations
- **Removable Media Control:** It is to be applied on controlling interactions to files on removable media storages only

2. Set Policy Severity level here. This option has significance, while using Grayteq Dashboard, wherein you can categorize threats based on their Severity levels.

3. Set to Create Snapshot from Host about Events which are blocked according to the Event Control

4. Set Policy's **scope**

- **On/Off-Net:** Policy takes effect irrespectively to the connection status between the Client and the Grayteq Security Server
- **On-Net:** Policy takes effect until there is live connection between the Client and the Grayteq Security Server

- **Off-Net:** Policy takes effect until there is NO live connection between the Client and the Grayteq Security Server
5. Set if Policy breach shall initiate Alert automatically.
 7. Check in the Use Time frame, if you want to use the Event Control in an appointed interval
 8. Set the Name of Event Control

NOTE: You have to assign new Event Control to an object for being applied!

Application Policy

With Application Policy, Grayteq Admins receive a new, easy to use security policy that enables them to manage application access policies on an efficient way.

Games, unauthorized browsers, instant messengers and other unwelcome applications can impact your business with their drain on employee productivity. Social media tools that are meant to aid people staying connected can also be a distraction. Create White-, Gray-, and Blacklists for all applications and decide how applications should operate or even being rejected. Whitelisted applications run smoothly, while unwanted or known harmful applications are denied by Blacklists. For millions of unlisted applications, setup Graylist actions to manage apps from not known sources or with no security clearance.

Application Policy Setup

1. Set **Application(s)** to control
 - Application name (eg. Calc.exe) or full path can be set also.
 - Set application's handling method by a three-way (BL/WL/WL+) switch, setting to which list (BL – Blacklist, WL – Whitelist, WL+ - Whitelist Plus) the application shall join.

COMMENT: Applications joined to Whitelist Plus, are going to be released from the list of Quarantine breaching applications, after a certain period of time.

EXAMPLE: Microsoft Office Outlook is a typical Whitelist Plus subscribeable application, while there is a need for accessing out of- and inside Quarantine documents in everyday work.

WARNING: Applications placed in %SYSTEM_DRIVE%\WINDOWS\ folder (like calc.exe) can be controlled by Event Control only.

2. Set additional settings for Application Policy
 1. Set **Severity level** for the given Application Policy. This setting has relevance in Dashboard, where you can find security breaches categorized by their severities.
 2. Set if **Snapshot** shall be created about the breaching attempt of the given Application Policy.
 3. Set Policy's **scope**
 - **On/Off-Net: Policy takes effect irrespectively to the connection status between the Client and the Grayteq Security Server**
 - **On-Net: Policy takes effect until there is live connection between the Client and the Grayteq Security Server**
 - **Off-Net: Policy takes effect until there is NO live connection between the Client and the Grayteq Security Server**
 4. Set if Policy breach shall initiate Alert automatically.
3. Set the name of Application Policy

Application Policy assignment

NOTE: You have to assign new Application Policy to an object for being applied!

Application Policies can be assigned to a Host or Host Group, or to Every Host. If more policies are assigned to the same Host or Hosts, Whitelist will be higher in policy priority meaning that if a Whitelisted Application Policy is assigned to a designated Host, it will set its applications as exceptions (making them whitelisted) from the applications of a Blacklisted Application Policy assigned to Every Host.

EXAMPLE: An Application Policy that denies skype.exe is assigned to Every Host and another Application Policy that allows the use of skype.exe is assigned to the Marketing Group hosts. In this case, skype.exe will run on the Marketing Group hosts, while remains denied on all others.

Graylist

Every application that is listed neither on Whitelists, nor on Whitelist Plus, nor on Blacklists is called Graylisted Application.

WARNING: Graylist is only available if there is at least one Black-, or Whitelist, or Whitelist Plus listed application in the system.

Graylist Management:

Graylist settings are at Server Properties:

- **Control:** Set if graylisted applications are to be managed according to Event Control related to them, or keep denied.
- **Test Mode:** Turn Application Policy test Mode on/off here. Test your Application Policies without risking system failure or breakdown by a failed policy setup.

IMPORTANT: All logs created in Test Mode are pseudo-logs that contain all log data of denied application running attempts, without applying denial for real. To separate Test Mode Logs from Real Denials (highlighted in Red), Test Mode Logs are highlighted in Orange.

Snapshot

With the help of this function policies can be created, and if those are realized, then a record will be made about the certain workstation. The importance of it is in the prove of circumstances. With Snapshot, it can be showed if the behavior caused any forbidden activity happened accidentally or intentionally. Snapshot can be freely combined with other protection functions (e.g.: Event Control, Quarantine).

Creating new Snapshot step-by-step

1. Select Events whereon Snapshot should be created. If there are no selected, it will be applied to all
2. Select Results, whereon Snapshot making is necessary. If there is no selected, it will be applied to all.
3. Select Users by whom the Snapshot making is necessary! If you not select any user, it will be applied to all.

TIP: By checking certain Users, these Users can be set to Exception Users. In this case all Events depicted within the present Policy, will be applied on all Users excluding the Exception ones.

WARNING: If unidentifiable User or Users are set, then these Users are going to be excluded during the inspection of the Policy.

4. Select Path and/or Files whereon the Snapshot making is necessary. Mask and negation can be used. If there is no selected, it will be applied to all

TIP: By checking certain Paths, these Paths can be set to Exception Paths. In this case all Events depicted within the present Policy, will be applied on all Paths excluding the Exception ones.

WARNING: If Exception Path(s) is set only, then blocking will be applied on all other (non-Exception) Path(s).

5. Set Target Paths to deny and its handling mode. This setting appears if any of the Copy or Move events were selected at the first wizard step.

Target Path handling setup options

1. **Exception:** Copy or Move is enabled for the Paths set only
2. **Standard:** Copy or Move is Denied for the Paths set only

6. Select Processes whereon the Snapshot making is referred. Mask and negation can be used. If there is no selected, it will be applied to all.

TIP: By checking certain Processes, these Processes can be set to Exception Processes. In this case all Events depicted within the present Policy, will be applied on all Processes excluding the Exception ones.

WARNING: If Exception Process (es) is set only, then blocking will be applied on all other (non-Exception) Process (es).

7. More options about Snapshot

1. Set Policy's **scope**

- **On/Off-Net:** Policy takes effect irrespectively to the connection status between the Client and the Grayteq Security Server
- **On-Net:** Policy takes effect until there is live connection between the Client and the Grayteq Security Server
- **Off-Net:** Policy takes effect until there is NO live connection between the Client and the Grayteq Security Server

8. Set the Name of Snapshot

NOTE: You have to assign new Snapshot to an object for being applied!

Device Control

Devices provide the possibility to establish access policy of general-purpose communication media. Such Devices can be Floppy drives, CD-, DVD drives, Infrared, COM, LPT, USB, Bluetooth, Wireless ports, etc. The most important feature of it is to block the Devices irrespectively of whether the Device is connected to the host or not, momentarily.

Device types:

- Floppy, ZIP Drive, A Drive and any other Devices similar with Floppy
- CD/DVD Writer Devices
- Infrared based Devices
- Bluetooth Devices
- IEEE 1394 FireWire
- Wireless (Wireless Zero Configuration (WZC))
- Serial Port based Devices
- Parallel Port based Devices
- Network Devices (Microsoft Windows Network)

- Network Devices (Novell Network)
- USB Storage Devices
- PCMCIA Adapters

Creating new Device Control step-by-step

1. Assign Device whereon you would like to apply a Policy
2. Set access rights of the selected Device
3. More options about Device Control
 1. Set Policy's **scope**
 - **On/Off-Net:** Policy takes effect irrespectively to the connection status between the Client and the Grayteq Security Server
 - **On-Net:** Policy takes effect until there is live connection between the Client and the Grayteq Security Server
 - **Off-Net:** Policy takes effect until there is NO live connection between the Client and the Grayteq Security Server
4. Set the Name of Device Policy

Warning: You have to assign new Device Control to an object for being applied!

Storage Control

For example: You have a general Policy which says, that every new Storages have a Read Only rights, here you can set a different right ex: a Normal right to a Storage with an allowed serial number or Hardware ID.

Creating New Storage Control

1. Set Mount Point, Serial and Hardware ID of Storage
 - You can select a Storage that is known already by Grayteq DLP. In this case click on **Add Remote** button and then select a Storage you would like to use. After you click on **Apply** button parameters of the selected Storage will be inserted into the Storage list.

WARNING: Mount Point, Serial and Hardware ID are mandatory!

WARNING: Serial number format is restricted. Valid serial number contains 4+4 digits hexadecimal characters separated with „-“ character. For example: 1234-ABCD

2. Select Policy of Storage Access
3. Settings
 1. Set Policy Severity level here. This option has significance, while using Grayteq Dashboard, wherein you can categorize threats based on their Severity levels.
 2. Set Policy's **scope**
 - **On/Off-Net:** Policy takes effect irrespectively to the connection status between the Client and the Grayteq Security Server
 - **On-Net:** Policy takes effect until there is live connection between the Client and the Grayteq Security Server
 - **Off-Net:** Policy takes effect until there is NO live connection between the Client and the Grayteq Security Server
 3. Set if Policy breach shall initiate Alert automatically.
4. Set the Name of Storage Policy

WARNING: You have to assign new Storage Control to an object for being applied!

Printer

Printer policies can be predefined. With their help it can be determined which printers can be used or blocked by a certain host. This feature can also be used in creation of Quarantines.

Creating new Printer Policy step-by-step

1. Set Printer Policy Setting
 1. Set to proceed the settled policy as negated

WARNING: If you set the negation, then selected Printer can be accessed only.

 2. Sets to create Snapshot if Blocked Event happens on the Host
 3. Set Policy Severity level here. This option has significance, while using Grayteq Dashboard, wherein you can categorize threats based on their Severity levels.
 4. Set Policy's **scope**
 - **On/Off-Net:** Policy takes effect irrespectively to the connection status between the Client and the Grayteq Security Server
 - **On-Net:** Policy takes effect until there is live connection between the Client and the Grayteq Security Server
 - **Off-Net:** Policy takes effect until there is NO live connection between the Client and the Grayteq Security Server
 5. Set if Policy breach shall initiate Alert automatically.
2. Set the Name of the Printers. If you not checked in the Negated option by the Printer Policy settings, here you will define the list of Blocked Printers. In Negated Policies, then these will be allowed Printers.
3. Set the Name of Printer Policy

WARNING: You have to assign new Printer to an object for being applied!

Quarantine

The Quarantine function is a special document area protection, which provides the possibility to create separate document spaces. Data movement can be controlled within these areas as well as beyond. It has importance to define approved users, applications, printers within the area, and specify the path to where the data can be exported. It has the ability to separate information both from Local and Domain Administrators, and the separation of the same application - runs within the Quarantine and outside of it -, e.g. copy content between two Word documents.

Creating New Quarantine step-by-step

1. Select the Path, which you'd like to handle as Quarantine area.
2. Set Quarantine settings
 1. **Create Snapshot** - Set to create Snapshot if a Blocked Event happens with a quarantined file
 2. **Advanced** - You can find these settings under New Quarantine>> Extended settings
 3. **Advanced Teamwork** - By using this option, all participants can be identified, for a given teamwork
 4. **Encrypted Data Transmission** - By this option, you can activate encryption for the current Quarantine

5. **Severity** - Set Policy Severity level here. This option has significance, while using Grayteq Dashboard, wherein you can categorize threats based on their Severity levels.
6. Set Policy's **scope**
 - **On/Off-Net:** Policy takes effect irrespectively to the connection status between the Client and the Grayteq Security Server
 - **On-Net:** Policy takes effect until there is live connection between the Client and the Grayteq Security Server
 - **Off-Net:** Policy takes effect until there is NO live connection between the Client and the Grayteq Security Server
7. Set if Policy breach shall initiate Alert automatically.
3. Set the Name of Quarantine Policy

Advanced Quarantine Policy Setup

1. Set Users with access to the Quarantine! If none is selected, it will be applied to all Users.

TIP: By checking certain Users, these Users can be set to Exception Users. In this case all Events depicted within the present Policy, will be applied on all Users excluding the Exception ones.

2. Set Processes which can access the Quarantine. If you not select any, it will be applied to all
3. Set Quarantine Data Flow access model
 - Select Quarantine **Access Policy**
 - Select if **Copy and Paste** is enabled for the content of the Quarantined documents
 - Select if **Drag and Drop** is enabled for the content of the Quarantined documents
 - Select **Data flow** model for the Quarantined documents file operations.
 - Set **Printer Control** for the designated Quarantine. Control whether Quarantined documents are printable to Printer Policy listed printers, or to Exception Printers only.

Encrypted Data Transmission Setup

1. Set Encryption/Decryption key.
Encryption key related options:
 - **Engage or Disengage** - Engage encryption keys to be used during encryption or decryption
 - **Key Security Classification** - is for data security classification level. A document can be decrypted by using a certain classification level key that classification level is at least equal or higher than the classification level of a key that were used during encryption. This function is not available in current version.
 - **Set Primary Key** - Sets the primary key that is in use for encryption

WARNING: You have to assign new Quarantine to an object for being applied!

Data Vault

Data Vault applies runtime, strong encryption on any document, file, folder, partition or even on full disc that remain protected if Grayteq DLP Client is turned off. Encryption and decryption occur in the background.

Data Vault requisite

Data Vault can be used only, if the designated host runs Grayteq DLP Client and have valid Grayteq license assigned to it.

COMMENT: Until there is no valid Data Vault license in your system, Data Vault Policy creation is unavailable.

WARNING: If the Data Vault license is subsequently installed, check/modify Administrator rights.

Data Vault Setup Steps

1. Set Paths to encrypt

WARNING: Paths-to-Encrypt have strict policies that may result Data Vault Policy failure if missed.

RULE: Path-to-Encrypt can be set on local, fixed drives with the setup of the full and exact path.

EXAMPLE: C:\Examples\Encrypt*

2. Set additional data Vault settings

1. Select if you want to set new Data Vault Encryption Key
2. Set New Encryption Key
3. Re-enter New Encryption Key
4. Select Encryption Algorithm

3. Set Data Vault name

WARNING: For taking the New Data Vault Policy in effect, it must be assigned to an object.

Data Vault Licensing

While Data Vault was developed as an independent encryption module for Grayteq DLP systems, its licensing is also independent from the Grayteq DLP Client licensing with numerous similarities in license management.

1. Click **Maintenance View's License** menu
2. With License Manager, **insert a Data Vault license** into the Security Server.

COMMENT: It's possible to use Client-Data Vault combo licenses where license insertion is to be completed once.

3. Select Client or Clients to activate Data Vault on.
4. Select **Data Vault license type** in menu bar and click **Activate**.

WARNING: Data Vault license can be assigned to an Client with valid Grayteq DLP license only.

5. Server Log notifies you about successful activation while the Client icon changes with a Data Vault icon on its bottom-left corner appeared.

WARNING: An assigned Data Vault license cannot be revoked. It can be redistributed to another Client by transferring the full Client license only.

COMMENT: At Client uninstall, Data Vault license assigned to it becomes redistributable.

Policy Group

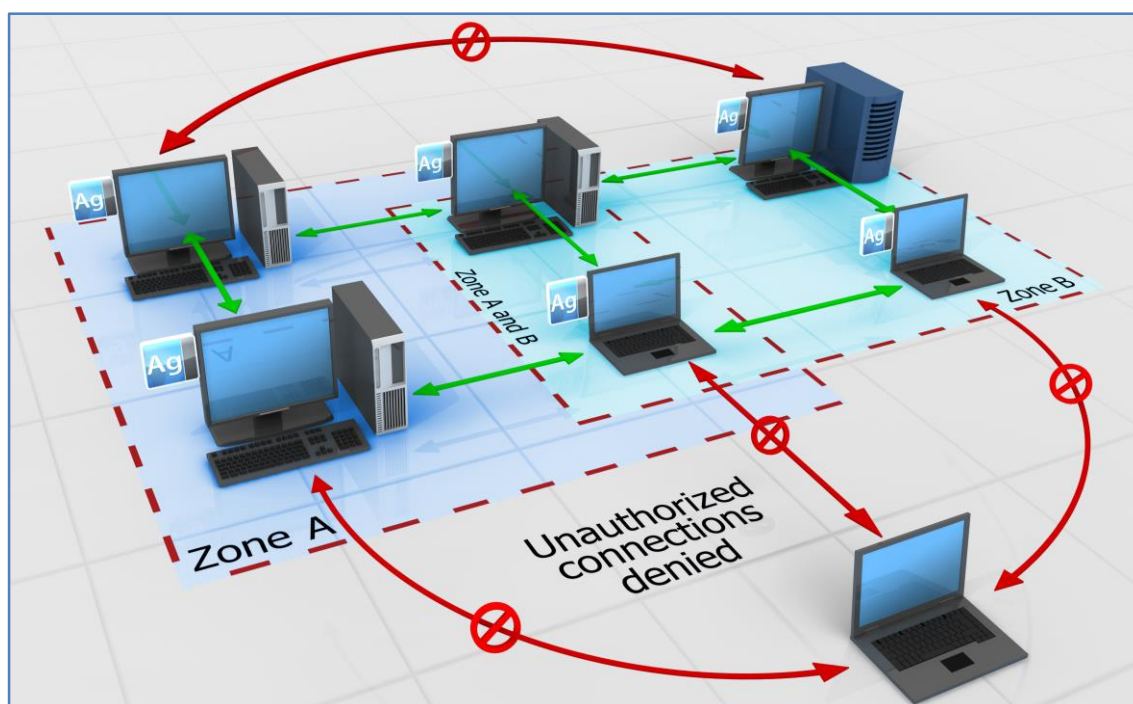
Policy Groups give help to group the pre-defined Policies, in order to assign them to Host or Host Group quicker and easier.

Creating new Policy Group step-by-step

1. Set the Name of Policy Group
2. Set the new Policy of Policy Group

WARNING: You have to assign new Policy Group to an object for being applied!

Intrusion Prevention



The dashed lines show the protection perimeter of Intrusion Prevention technology. With a single setup, it makes possible to access files, shares, folders stored on a given computer only for those computers within the network, which ones have any Grayteq product with Intrusion Prevention function.

With this functionality two separated computers are able to communicate only, if both have any Grayteq product with Intrusion Prevention function, running at the time of communication, and have at least one matching Intrusion Prevention authentication key assigned.

Using this technology, computers within the Intrusion Prevention and files, folders, drives stored on it, are unavailable for computers illegally connected to the network. Intrusion Prevention can be created as an individual Policy, and then be assigned to Hosts in order to make separating different company groups easier.

This function provides possibilities to create unlimited number and flexible separated zones within the organization. These ones can be independent from each other or overlapping either.

Creating new Intrusion Prevention step-by-step

1. Set Identifier Key of Intrusion Prevention
2. Set Policy Severity level here. This option has significance, while using Grayteq Dashboard, wherein you can categorize threats based on their Severity levels.
3. Set Policy's **scope**
 - **On/Off-Net:** Policy takes effect irrespectively to the connection status between the Client and the Grayteq Security Server
 - **On-Net:** Policy takes effect until there is live connection between the Client and the Grayteq Security Server
 - **Off-Net:** Policy takes effect until there is NO live connection between the Client and the Grayteq Security Server
4. Set if Policy breach shall initiate Alert automatically.
5. Set the Name of Intrusion Prevention

WARNING: You have to assign new Intrusion Prevention to an object for being applied!

Hosts, Host Groups, Every Host, Host Statistics

Here you can see the list of managed Hosts and created Host Groups in hierarchy. You can manage an Client, turn on the Silent Mode and control the access of new Storages.

Creating new Host Group step-by-step:

1. Set the name of new Host Group, and you can give more details in Description field about it
2. Assign Host to this newly created Host Group

Host Dependencies, Statistics

To set the Hosts items of a Host Group, you have to drag selected Host icon on the name of Host Group (Drag and Drop). The Host name will appear under the Host Group. You can see it at Dependencies also.

Host settings

To access settings of any Host, double-click on it.

1. Set the Client's state and running mode
2. Set handling policy of newly attached Storages
 1. **File system:** Set a newly connected Storage (with file system) to be handled as New Storage, compared to the default Storage created at first installation of the Client.
 2. **Access:** Set access rights to a newly connected Storage (with file system)
3. If you want to configure a Storage that has been connected already, select the Storage on Host to configure, watch its properties then set its options
 1. **Access:** Set access rights of newly attached Storages (with file system).
 2. **Access Mode:** Set access rights which should be permanent or just for one time only.
 3. **State Recovery:** Set accesses for the designated Host, while restores its original access after the expiration of the period set priory. The designated Administrator will be emailed about the interactions occurred on the given Storage.
4. You can give more information about the Host in Description field.

Users, User Groups, Every User

Here you can see the list of managed Users and User Groups in hierarchy. You can create new User or User Group and/or you can migrate it from your existing Active Directory.

Creating new User step-by-step:

1. Set the name of the new User and you can give more information about it in Description field also

WARNING: The icon of the created User will be different from the icon of the User listed by the Security Server.

2. Order this newly created user into structure

User migration

Security Server creates the list of User from the Active Directory. The result will contain each Users and User Groups of that domain, whereon the Grayteq DLP Security Server presents.

Creating new User Group step-by-step:

1. Set the name of the New User Group and you can give more information about it in the Description field also
2. Assign any Users to the given User Group

User dependencies

Get User dependency information about any user in Policies view. Drag and drop the designated User to the Navigation Panel and check User assigned Policies.

Maintenance view

Accessible functions by Maintenance view:

- [Install](#)
- [License](#)
- [Update](#)
- [Server Log](#)
- [Servers](#)
- [Operators](#)
- [Archives](#)
- [SYSLOG settings](#)
- [SQL settings](#)
- [Server Properties](#)

Install

To accessing Install Logs, double-click on that Host which Host's Install Log you would prefer to view

Install Logs provide additional information and events occurred during the installation on a selected workstation.

WARNING: Install Log will be prepared in that case only, if the Installation has been finished successfully or ended with special kind of Failure notice.

License

WARNING: If Grayteq DLP Client runs without License will not apply any policies (except Log Filters), and the Log entries content will not be displayed.

License file contains all Grayteq DLP Client licenses purchased.

Licensing for the given Grayteq DLP Clients are as follows:

1. **Insert license** into the Grayteq DLP system, with License Manager. Set the number of distributable Clients here.
2. **Assign License** to the designated **Host** or **Hosts**

WARNING: Client icon color is informative for the Operator: if it's gray, there is no License assigned.

Update

You can install Upgrades to selected Hosts or Host Groups. Review Grayteq DLP Client version and find information about version history of certain Hosts also.

Server Log

Server Log provides continuous status information on Security Server operations; displaying informal messages on the procedures performed by the Security Server in real-time.

More information

- Error messages can be seen with Support ID in order to make troubleshooting easier.
- You can gain information about the operation of Grayteq DLP Security Server with the button of the left part of Grayteq DLP Security Orchestrator, where the Server Log panel constantly displays information.

- This panel displays real-time information about operation feedback, events on the server, Status Information that has a white background; and error messages that appear with red background color.
- On the panel toolbar, Scroll button can be used to enable the most recent event to be displayed. If this option is switched off, the list of events will not scroll when new event occurs.
- You can delete any previous events clicking on the Clear button. If you click the Reset Column button, columns can be reverted to its default.
- Panel displays information sorted into columns. Time of the event can be found in the Time column. Category column contains the category of the event. In Description field, you can see a description of the event that - if the Operator initiated the event - contains Operator name. In Support ID column, you can find an ID that can be used in case of an error, to find further information on Grayteq DLP support pages about the error and related troubleshooting.

Servers

Servers store incoming event logs and defined Policies, as well as it command all Clients to manage the network properly. Several Security Servers can be managed with a single Security Orchestrator, or several Security Orchestrators can be connected to a single Security Server. Furthermore, the relevant statistical information on the Security Server can be queried from here.

Operators

Different process- and security level related activities can be separated from each other. Different rights can be assigned to certain Operators, and it is possible to separate e.g.: operation tasks of the information technology area from the report reading rights of the people responsible for the security.

Archives

Incoming event logs are located in a data storage structure specially developed for this purpose. Event logs archived automatically based on determined size and time. This function increases in significance with ongoing operations. Constant personal control is not necessary to keep the performance of the Security Server at an appropriate level despite of continuously increasing logs. Information can be queried directly in the archived data.

Available information about an Archive

- **Name:** Archive name
- **Path:** Archive path
- **Elements:** Number of elements in Archive
- **State:** Archive state
- **First element:** Date of first element in Archive
- **Last element:** Date of last element in Archive
- **Unknown Elements:** Number of elements in Archive, belonging to unknown hosts
- **List:** Shows elements in list

SYSLOG Settings

Using SYSLOG support, the operational resource's needs and costs can be reduced further, additionally the integration to a third-party centralized remote management, and error handling or alert system can be executed easily. SYSLOG contains the full path of objects, e.g. using HP OpenView Operations; the event occurrence can be represented in Service Grid without developing any additional Smart Plug-In. Third parties' products without the need of completeness: HP OpenView, IBM Tivoli, Cisco MARS, Novell Nsure Audit, etc.

SQL Settings

With the help of this the personally developed database technology can be redeemed with an existing and centrally managed SQL database that already has some pre-configured operational tasks (e.g. safe storing, saving etc.). Supported database: Microsoft SQL Server.

Supported Databases:

- Microsoft SQL Server (SQL Server 2008 R2 as well)
- PostgreSQL Server in unicode mode
- PostgreSQL Server in ANSI mode
- Oracle 10G Database Server

Server Properties

1. If you want to set a different picture for the Security Server, you can browse for a new one
2. Communications

1. **Base port:** You can see the communication port of the Security Server here
2. **Port Number:** You can see the number of the communication ports here
3. **Server State Repeat Time:** Set the rate of the minutes when the Security Server should send status report to the Security Orchestrator

COMMENT: To avoid communication problems, - in case of Grayteq DLP Server recognizes that connection to its external database is lost – reconnect to the database occurs here. The system notifies the designated Administrators in email, if reconnection attempt fails.

3. Hosts settings

1. **New Storage Mode:** Set when a newly attached Storage (with file system) should be handled as a New Storage, compared to the default Storage created at the first installation of the Client
2. **Storage Access:** Set default policy of the Storage handling
3. **Client in Silent Mode:** Set running mode of the Client
4. **Host Lost Days:** Set that the Host that is not sending any Events, after how many days will be shown as a lost Host. You can see different icons in the Security Orchestrator in front of the Host' name depending from the Host's state.
5. **Severity:** Set „New Storage Action” related threats' Severity level here. This option has importance, while using Grayteq Dashboard, wherein you can categorize threats based on their Severity levels.
6. **Off-Net Timeframe:** Set the timeframe when the Clients turn to Off-Net mode after.
7. **Set and Display:** Set primary, secondary and third Host name ID to display.

COMMENT: This setting can be changed at anytime with no affect to log storing. Log displaying is affected only.

4. Policy related settings

1. **Application Policy Graylist Severity:** Set Graylist severity here. This setting has relevance in Dashboard, wherein you can prioritize breaches by severities
2. **Block Graylisted Applications:** Set all Graylisted Applications blocked. If it's not set, Graylisted Applications can be managed by Event Controls only.
3. **Test Mode:** Turn Application Policy test Mode on/off here. Test your Application Policies without risking system failure or breakdown by a failed policy setup.

IMPORTANT: All logs created in Test Mode are pseudo-logs that contain all log data of denied application running attempts, without applying denial for real. To separate Test Mode Logs from Real Denials (highlighted in Red), Test Mode Logs are highlighted in Orange.

5. Maintenance related settings

1. **Log Time Threshold:** Set the maximum range of time, when it has to write the log on a hard drive
2. **Log Event Flush Size:** Set the maximum number of the Events after it has to write them on a hard drive
3. **System Backup Schedule:** Set Autosave timeframe for the Security Server
4. **Init in OS event log:** Set if Security Server init logs are to appear in operating system logs.
5. **Warnings in OS event log:** Set if Security Server warning messages are to appear in operating system logs.
6. **Errors in OS event log:** Set if Security Server error messages are to appear in operating system logs.

COMMENT: Section 4-5-6 are important at service level startup of the Grayteq DLP Security Server, while console window is not available wherein proper operations of the Security Server could be followed.

6. Notifications

1. **E-mail sender:** Set the e-mail address of the sender who sends letters by the Security Server
2. **Mail Server:** Set default mail server for sending e-mails. IP address can be used
3. **SMTP port:** Set the SMTP port of the default mail server
4. **E-mail subject:** Set your own note which you want to see in the subject line
5. **Report mode:** Set format of the Reports

7. Performance

1. **Multi processor:** You can set here for the Security Server to use more processor
2. **Snapshot frequency:** Set frequency of Snapshot making. Higher security settings can cause decreasing in the performance
3. **Check Time in Minute:** Set Security Server by how many minutes controls the a cascade spool
4. **Percent of Cleanup:** Set Security Server by how many percent cleans up the cascade spool
5. **Auto Report and Alert Max Size:** Set the maximum size of the storage capacity of the Auto Reports and Alerts on the Security Server
6. **Current Percent:** It shows the actual capacity of the storage of the Auto Reports and Alerts on the Security Server
7. **Update Package Max Size:** Set the maximum size of the storage capacity of the Update Package on the Security Server
8. **Current Percent:** It shows the actual capacity of the storage of the Update Package

8. Troubleshooting

1. **Time Index Check:** Force Security Server to check and repair chronology of log files at the next start
2. **Consistency Check:** Force Security Server to check and repair time consistency of log files at the next start

9. Archives

1. **Day:** Set how many days after the first install or last archives Security Server has to archive
2. **Max Size:** Set size of log files (MByte) by reaching it Security Server will archive anyhow
10. If you want you can give more information in the Description field

Security Server command line switches

- `/reconfigurepath`
Upon successful authentication, Administrator right Operator can reconfigure the storing location of System settings backups (e.g. Grayteq Security Server config.xml and licenses file(s)).

NOTE: Security Server will continue to log into the default folder if the folder(s) determined here is (are) not available.

- `/clientrestore`
It means to start Security Server in Client Restore mode. In this mode Security Server uses DNS Server to identify Host Clients, but the identification algorithm built in Client (Security Orchestrator). With this switch, problem by updating the Client's list - caused by an occurring network problem - can be restored.

NOTE: In order to ensure more efficient operation, it is suggested to execute the "ipconfig/flushdns" command on the Security Server Host before running.
WARNING: DNS-based identification can cause performance loss in the operation of the Security Server. Identification uses it until all Clients log back to the Security Server. This switch is for a special troubleshooting. Before using, in case, consult with the Support Team!

- `/Help or /?`
Shows a brief description of the commands above.

Support ID

Recently updated Support IDs

By Support IDs the frequently occurred errors can be recognized and fixed.

Support ID appears in the Server Log, and consists of the following elements:

- **Number:** Number of Support ID
- **Short description:** Short description of the symptom and/or the error
- **Long description:** Long description of the symptom and/or the error
- **Cause:** Cause of the symptom and/or the error
- **Solution:** Possible solution for the symptom and/or the error
- **Version:** Version number of the released software whereon the symptom and/or the error is fixed

WARNING: Support ID does not contain version information such as the symptoms and/or errors that are general by default, and don't refer to irregularities related to the operating circumstances of the Grayteq DLP system. The Licensor issues hotfix developments within the lifecycle of the given software version to avoid unwanted symptoms and/or errors.

Support IDs

10001

Short description	Memory allocation error in the Security Server.
-------------------	---

Long description	Security Server couldn't process the Client's request, displayed in the message, because couldn't allocate the required amount of memory.
Cause	Security Server's available physical memory undersized possibly.
Solution	For appropriate sizing of the Security Server Install Guide gives help.
Version	N/A

10101

Short description	Name resolution error.
Long description	Security Server couldn't identify the connecting Client or Security Orchestrator Host's name. Without name resolution the connecting Host cannot be identified unambiguously.
Cause 1	DNS service in the network is not configured correctly.
Solution 1	In addition to configure the DNS server, may be required to run an "ipconfig /flushdns" command the Security Server's computer.
Cause 2	Security Server is overloaded, the Clients disconnect due to timeout problems.
Solution 2	For appropriate sizing of the Security Server Install Guide gives help.
Version	N/A

10102

Short description	IP address resolution error.
Long description	Security Server couldn't resolve the connecting Client's or Security Orchestrator Host's name therefore couldn't identify it. Without IP address resolving the connecting Host could not be verified.
Cause 1	There is an IP conflict between one or more Hosts, which have Client running on it.
Solution 1	In case of static IP addressing the Hosts runs the Clients must have IP address assigned uniquely.
Cause 2	Security Server is overloaded, Clients are disconnecting due to timeout problems.
Solution 2	For appropriate sizing of the Security Server Install Guide gives help.
Version	N/A

10201

Short description	Obsoleted function access attempt.
Long description	A Client requested an obsoleted function request from the Security Server, which is not supported anymore. The Security Server denied the request.
Cause	One or more Clients with version less than 2.0 are present in the network on Hosts.
Solution	Upgrade all Clients to version 2.0 at least. You can download the latest version from here.
Version	N/A

10301

Short description	Synchronization error in the Security Server's Policy handler.
Long description	Synchronization error occurred in the Security Server's Policy handler. Policy in the error message was deleted while one or more Security Orchestrator was refreshing Policies.
Cause 1	One or more Security Orchestrator tried to use the same Policy simultaneously.
Solution 1	Repeat requested operation.
Cause 2	Another Operator had deleted policy meanwhile.
Solution 2	Please wait, while the Security Orchestrator refreshes the Policy list.
Version	N/A

10302

Short description	Client identification error.
Long description	An Client computer requested a function in the Security Server that requires identification. The Security Server denied the request due missing identification.
Cause	Security Server is overloaded; the Client closed the connection before the identification process finished.
Solution	For appropriate sizing of the Security Server Install Guide gives help.
Version	N/A

10402

Short description	Synchronization error in the Security Server.
Long description	Security Server's synchronization module referenced to an invalid object, this can cause problems in the inner logic of the

	Security Server, and incorrect operation.
Cause	Security Server's version is outdated.
Solution	Update the Security Server. You can download the latest version from here .
Version	N/A

10403

Short description	Synchronization timeout error in the Security Server.
Long description	Security Server couldn't process its current operation in the allowed time frame. This may cause performance loss or malfunction.
Cause	Security Server's version is outdated.
Solution	Update the Security Server. You can download the latest version from here .
Version	N/A

10501

Short description	The event logging system detected a bad log file size during self-tests.
Long description	The event logging system detected a bad log file size during self-tests. The Security Server corrected the error automatically.
Cause 1	There was an error during writing of the event log file.
Solution 1	Verify if there is enough free storage for the event log files. Verify if any blocking Policy was assigned to the Host that runs the Security Server.
Cause 2	Security Server was stopped incorrectly. (e.g. power failure)
Solution 2	Stop the Security Server always from the Security Orchestrator.
Version	N/A

TIP: It is recommended to perform Consistency Check on the event log files.

10502

Short description	File system error in Consistency Check process.
Long description	Security Server detected a file system error while processing Consistency Check and couldn't check/repair the event log file.
Cause	There was an error during the writing of the event log file.

Solution	Verify if there is enough free space for the event log files. Verify if any blocking Policy was assigned to the Host that runs the Security Server.
Version	N/A

10503

Short description	The event logging system has detected incorrect event log data during self-tests.
Long description	The event logging system has detected incorrect event log data during self-tests. The incorrect data entries had been removed from the event log.
Cause 1	There was an error during the writing of the event log file and error was detected by Security Server's self test algorithm.
Solution 1	Restart the Security Server with the Consistency Check option.
Cause 2	There was an error during the writing of the event log file.
Solution 2	Verify if there is enough free storage for the event log files. Verify if any blocking Policy was assigned to the Host that runs Security Server.
Version	N/A

10601

Short description	Time Index system has detected an unrecoverable error in the course of the automatic self-test.
Long description	One or more file of Time Index system cannot be created or opened. Security Server requires these files to keep its logs in time order for the queries.
Cause	There was an error during the writing and/or reading of the event log file.
Solution	Verify if there is enough free storage for the event log files. Verify if any blocking Policy was assigned to the Host that runs Security Server.
Version	N/A

10602

Short description	Time Index database was damaged.
Long description	Time Index database was damaged because of previous error (e.g. power failure), and there are incorrect references in Time Index files. Incorrect references may cause event log inconsistency during event logging or reporting.
Cause 1	Time Index file was damaged during a previous run of the

	Security Server.
Solution 1	Restart Security Server with Time Index Check option.
Cause 2	Security Server's event log files and Time Index files mismatch (e.g. error during backup restore).
Solution 2	Restart Security Server with Time Index Check option.
Version	N/A

10603

Short description	Error in the integrity of String Index files.
Long description	Error in the integrity of String Index files. One ore more String Index data is unavailable for the Security Server. Security Server continues its work correctly, but "INVALID" strings may appear in the logs.
Cause	One of the Security Server's String Index files had been damaged.
Solution	Restart Security Server with Consistency Check option.
Version	N/A

10702

Short description	Security Server cannot load the dbghelp component.
Long description	Security Server's error handler module requires the dbghelp.dll component to identify the location of any error has occurred during its operation exactly. If any unhandled exception has occurred in the Security Server, this component helps locating the source of error for the Support Team.
Cause	The dbghelp.dll is not present on the computer that runs the Security Server.
Solution	You can download the necessary component from here: http://www.microsoft.com/downloads/release.asp?releaseid=30682
Version	N/A

10703

Short description	File opening error.
Long description	Security Server cannot open or create a file that required for its operation. The error code and the error description (these information are from the Security Server's operating system) are included in the error message. If the error occurs numerous times the Security Server shuts down itself, to prevent any damage in the event log system.
Cause	The user runs the Security Server doesn't have sufficient rights to create the specified file.
Solution	Set permission to Full Control on the file in the error message for the Security Server running user.
Version	N/A

10704

Short description	Missing or duplicated identifier is in Security Server's unique identifier list.
-------------------	--

Long description	Security Server found a missing or duplicated identifier in Security Server's configuration file.
Cause	N/A
Solution	Please, contact the Support Team.
Version	N/A

10705

Short description	Thread stopping error.
Long description	There are one or more long operations in process while a Security Server stop request has arrived. The stop request cannot be processed without damaging the integrity.
Cause	Security Server was stopped, but not from the Security Orchestrator. (E.g.: terminating the Security Server's process directly on the computer that runs it.)
Solution	Stop the Security Server always from the Security Orchestrator.
Version	N/A

10706

Short description	License system violation.
Long description	Security Orchestrator has requested an obsoleted (and unsupported) Client activation. The Security Server denied request.
Cause	One or more Security Orchestrator can be found on the network with a version less than 2.0, and one of them tried to activate an Client License.
Solution	Upgrade Security Orchestrator to version 2.0 at least. You can download the latest version from here.
Version	N/A

10707

Short description	Invalid event log directory.
Long description	Previously set event log directory inaccessible for the Security Server. Logging will continue into the default event log directory.
Cause 1	Partition for the event logs is full.
Solution 1	For appropriate sizing of the Security Server Install Guide gives help.
Cause 2	Remote (network) event log path inaccessible.

Solution 2	Assure that the event log directory is always reachable and writable by the Security Server during the entire running time.
Version	N/A

10708

Short description	Event log cache was turned off temporarily.
Long description	Event log cache was turned off temporarily for the current query operation.
Cause	Security Orchestrator's query request has occurred at the same time as the scheduled cache optimization.
Solution	This is not an error, but the processing time of the current query can increase slightly.
Version	N/A

10901

Short description	Install package (.gup) upload file error.
Long description	Install package (.gup) cannot be uploaded to the Security Server because the update packages' Cascade Spool directory is not writable.
Cause	Storage is full whereon the update packages' Cascade Spool directory is located.
Solution	For appropriate sizing of the Security Server Install Guide gives help.
Version	N/A

10902

Short description	Install package uploading connection error.
Long description	Install package cannot be uploaded into the Security Server because the update package has damaged during the uploading process.
Cause	Network errors caused data loss during the uploading process.
Solution	Repeat the uploading process. If the error continues, please contact the Support Team.
Version	N/A

Remove Client

Manual Remove

- Stop running Client from Security Orchestrator
- Open a new command-line with administrator rights (Run >> cmd)
- Navigate to %ProgramFiles%\Grayteq\DLP\Client\ folder and enter the following:
 - **grclsvc.exe uninstall**
- Restart your computer

NOTE: In case of the Client cannot be stopped via Security Orchestrator, then run the command above in Safe Mode.

Remove Client via Security Orchestrator

Clients can be remotely uninstalled from Security Orchestrator using live connection between the Security Server and the designated Client. At this step, command-line step are completely avoidables, license are transferred back to the License Stash, wherefrom redistributables to the remaining period of time to other Hosts.

COMMENT: It's expedient to uninstall Client on the Security Orchestrator, if the Client is de facto has been uninstalled manually from the Host, or the Host suffers from hardware malfunctions that keep it in inoperating state, because in this case – in opposition to license transfer - previous licenses remain visible.

Client uninstall steps

1. Click **Policies** view, then select **Hosts**
2. Select Client to uninstall
3. Click Uninstall, or select Uninstall in right-click menu.

If the given host runs Grayteq Client, it stops and uninstall automatically, with no user interaction needed.

WARNING: For completing uninstall, Host reboot is needed at this case.

Troubleshooting

This chapter includes the following sections:

- [Known compatibility Issues](#)
- [Remote Installation](#)
- [Slowdown](#)
- [Application Logs](#)
- [Unreasonable local logging](#)

Known compatibility Issues

Computer crash

Symptom

With Grayteq DLP Client installed, computer crashes while the user click on Taskbar's Volume icon's „Mute” option, or presses „mute” button on keyboard.

Solution

Update SoundMax driver on HP notebooks listed below

- HP 2133 Mini-Note PC
- HP 2140 Mini-Note PC
- HP Compaq 2230s Notebook PC
- HP Compaq 6530b Notebook PC
- HP Compaq 6530s Notebook PC
- HP Compaq 6531s Notebook PC
- HP Compaq 6535b Notebook PC
- HP Compaq 6535s Notebook PC
- HP Compaq 6730b Notebook PC
- HP Compaq 6730s Notebook PC
- HP Compaq 6735b Notebook PC
- HP Compaq 6735s Notebook PC
- HP Compaq 6830s Notebook PC
- HP EliteBook 2530p Notebook PC
- HP EliteBook 2730p Notebook PC
- HP EliteBook 6930p Notebook PC
- HP EliteBook 8530p Notebook PC
- HP EliteBook 8530w Mobile Workstation

HP EliteBook 8730w Mobile Workstation

If your notebook model is listed above, update your SoundMax sound card driver to the driver on the following URL:

<http://h20000.www2.hp.com/bizsupport/TechSupport/SoftwareDescription.jsp?lang=en&cc=us&prodTypeId=321957&prodSeriesId=3781677&swItem=ob-68619-1>

Remote Installation

Failed remote installation

Symptom 1

No Endpoint status.

Solution 1

Check the given computer if it is turned on and have access to local network.

Symptom 2

No Endpoint or Access Denied status.

Solution 2

Check if the computer has the required Admin shares and the user who runs Grayteq DLP Security Server can access them.

NOTE: For Example: By entering the dir \\computername\C\$ command you can get the information if the C\$ Admin Share is available or not. In case the appropriate shares exist but unavailable, check the firewalls of the given workstation and on network if the necessary ports are opened.

IMPORTANT: In case of errors 'No Endpoint' and/or 'Access Denied', Grayteq DLP Security Server attempts to execute the install process in every 10 minutes. It is not needed to order it again, because after fixing the error, the Security Server attempts to execute the install process again automatically.

In case of completely unsuccessful installation

Contact the Support Team. The following information will be asked for - so please, get them prepared:

- Status of the unsuccessful installation
- Exact Host name
- Detailed Installation Log
- The Security Server's Status Log

Slowdown

Security Server slow down

Symptom

The Host runs Security Server slows down significantly. The Security Server needs a lot of CPU time for its operation, the system resources are overloaded and/or the network communication slows down.

Cause

The Security Server chronologically orders the log files received from the Clients continuously. Sometimes it can happen that large amount of Clients (even thousands or more) start to upload their locally stored log files at the same time. In this case, the Security Server can slow down, as it creates the chronological order of the log files.

Solution

It is not an error. As soon as all of the Clients have uploaded their locally stored log files to the Security Server, the symptom does not exist anymore.

EXAMPLE: A partial segment of corporate network loses its connection with the other segments of the network, even with Grayteq DLP Security Server. In case the Clients immediately start to log locally. After fixing the network problem, each Client attempts to upload the locally stored log files to the Security Server.

Client slow down

Symptom

The computer that runs the Client slows down significantly. The Client needs a lot of CPU time for its operation, the system resources are overloaded and/or the network communication slows down.

Cause

An inappropriately set policy has been assigned to the Client.

NOTE: During the development of the Client, the low resource consumption had top priority. Due to this, it is not allowed to cause observable slowdown for the user in the normal operating environment and circumstances.

Solution

Check the Policies assigned to the given Host, or rather which Policies from those take Snapshots.

TIP: You can see it on the Monitor page also; where on the Snapshot icon appears beside the Events.

Set a lower level for Snapshot creating frequency by the Server properties.

Check if the Snapshot is really required if the given event occurs. It is possible that the resource required for it is out of proportion considering the value of information.

Security Orchestrator slow down

Symptom

The computer that runs the Security Orchestrator slows down significantly. The Security Orchestrator needs a lot of CPU time for its operation, the system resources are overloaded and/or the network communication slows down.

Cause

The Security Orchestrator stores all of query data in its memory, in order to ensure their availability at all times. It can happen that several queries with large quantity of elements run parallel (Report, Auto Report, etc.). In this case, the Security Orchestrator starts to allocate the necessary quantity from the available memory. It causes the slowdown of the Security Orchestrator and the computer also.

Solution 1

- Close one or more opened Report
- Close one or more opened FLT
- Close one or more opened SLT
- Close one or more opened Auto Report
- Close one or more opened Alerts

Solution 2

- Stop the Real-time monitoring feature on the Monitor page.
- Reduce the depth of the monitor rows on the Monitor page.

Application Logs

Security Server Error Log

The Security Server has built-in error handling. In case of an application error, the error handling generates a log file. The log file contains the reason of the given error; furthermore a detailed memory map about the moment the application error occurred. The default location of log files: **%ProgramFiles%\Grayteq\DLP\Server\ErrorReport**

During troubleshooting, these files help the work of the Support Team.

Security Server Status Log

The Security Server has a built-in Status Log. This contains all of the handled errors. This log file can be found as a default: **%ProgramFiles%\Grayteq\DLP\Server\Log\GrayteqLogEvent.log**

During troubleshooting, this file helps the work of the Support Team.

Client Error Log

The Client has built-in error handling. In case of an application error, the error handling generates a log file. The log file contains the reason of the given error; furthermore a detailed memory map about the moment the application error occurred. The default location of the log files: **%ProgramFiles%\Grayteq\DLP\Client\ErrorReport**

During troubleshooting, these files help the work of the Support Team.

Security Orchestrator Error Log

The Security Orchestrator has built-in error- handling. In case of an application error the error handling generates a log file. Logs about the handled and non-handled errors are in the default-operating folder: **%APPDATA%\Grayteq\DLP\error.log**

Unreasonable local logging

Symptom

One or more Clients log locally, while the computer that runs the Client have access the Security Server.

Cause

It is a typical example for uploading the log files in large quantities to the Security Server. Grayteq has a built-in protection mechanism. Due to this, Grayteq does not allow for the Security Server to occupy an excessive resource from the computer or its hardware running the Security Server. The protection mechanism detects if occupies an excessive resource to process the data coming from the Client. In this case, it signs to the Client to log locally and don't send further data to the Security Server.

NOTE: The message 'Temporary suspending message processing' notifies you about it in the Security Server Log.

TIP: It can be a solution; if Hosts run Clients can be turned on for the periods with less loading (e.g. for nights). In this case the Security Server can process data, which were stored locally by the Clients.

Solution 1

It is not an error. The log data are not lost, just stored locally and if the overload ends, they will be sent to the Security Server.

Solution 2

Overload reason is that Grayteq system runs without Log Filters or with misconfigured Log Filters. Check the configuration!

TIP: It is possible; that a new application has been installed in the organization whereto no Log Filter had been created.

Solution 3

Security Server overload can be caused by misconfigured hardware. The Installation Guide helps to configure Security Server correctly.

Disaster Recovery

This chapter includes the following sections:

- [Introduction](#)
- [Data](#)
- [Disaster types](#)
- [Error handlings](#)

Introduction

The goal of this document is to provide help to restore Grayteq DLP as soon as possible, in case of malfunctions of the running environment, respectively the modules of Grayteq DLP also.

Data

System datasheet

Please, fill the table below, if you find some irregular system behavior.

Computer information, which runs Grayteq DLP Security Server:	
Name of the computer (FQDN) and its IP address:	
Installation path:	
Access path of log and archive folders:	
Backup method (monthly/weekly/daily):	

Data to backup

For System protection and easy recovery of each component of your Grayteq DLP system, it is important to backup system configuration and log files on a regular basis.

WARNING: Backup configuration and log files regularly as follows:

- Grayteq DLP Security Server configuration file (GrSrCfg.dat file),
- Grayteq DLP Security Server license file (GrSrLic.dat file),
- Grayteq DLP Security Server Storage database file (SysConfig.dat),
- Content of Log and Archive folders.

TIP: Backup folders and files are stored in %ProgramFiles%\Grayteq\DLP\Server folder, by default. It is recommended to store log and archive folders on a different drive, separated from system files.

Disaster types

- Misconfigured Client Policies
- Damage or destruction of running environment
- Loss of function

Misconfigured Client Policies

The typical reason of this type of disaster is, whenever based on a personal fault, the policies had been created generating an error on computers which runs Grayteq DLP.

COMMENT: Grayteq DLP Clients operate in the Operating System core (kernel). Every Client sends requests to the Grayteq Security Server in every two seconds, to check policy changes.

A policy is to be considered as false in case it prohibits the proper usage of the Client running computer.

Solution method: Removing Policies

At Client stopping, whereas Grayteq DLP Security Server runs, remove the falsely set policy(s) (delete it/them) from such computers or users which ones were assigned to.

Restart the incident related computers. Grayteq DLP Clients at the startup connect to Grayteq DLP Security Server first to download actual policies. When all falsely set policies have been removed, the computers will run properly.

In case an error affects the Client, which runs the Security Server and it is not possible to login to Grayteq DLP Security Server then the following steps may help in troubleshooting:

- Start the computer, which runs the Security Server, in “Safe Mode” (F8).
- In Control Panel / Administrative Tools / Services panel set Grayteq Client Service’s startup mode to “Manual”.
- Restart the computer, at this time in normal mode.
- The computer will start properly and it will be possible to log in to Grayteq DLP Security Server.
- The error-causing policy can be removed from Grayteq DLP Security Orchestrator.
- Set Grayteq Client Service’s startup mode back to “Automatic”. Restart the computer.

Damage or destruction of running environment

These types of disasters are typically in accordance with physical problems, which ones emerge in the running environment of Grayteq DLP Security Server. Partial or total failure of the computer, network breakdown, or partial or total damage of configuration data caused by a fatal hardware error are to be considered as such disasters.

Hardware errors

The cause of this type of disaster is a malfunction of one or more hardware components of the computer runs Grayteq DLP Security Server. Based on hardware errors Grayteq DLP Security Server is need to be installed to a new computer.

Restoring Grayteq DLP Security Server within the same environment

Pre-installation, check the followings:

- Up to date backup copy of GrSrCfg.dat file is available.
- Up to date backup copy of GrSrLic.dat file is available.

WARNING: Grayteq DLP Clients identify Grayteq DLP Security Server based on its IP address and FQDN name; therefore it is important to install the new running environment under the same IP address and FQDN name.

- Install Grayteq DLP Security Server in the new running environment.

WARNING: It is important to have the same installation path as per the previous (e.g. “old”) system.

- Copy GrSrCfg.dat and GrSrLic.dat files to %ProgramFiles%\Grayteq\DLP\Server\ (or into the folder wherever the software were previously installed) folder after finishing the installation.

After this, the system will operate based on the previous (e.g. “old”) configuration.

Restore Grayteq DLP Security Server into changed environment

Pre-installation, check the followings:

- Up to date backup copy of GrSrCfg.dat file is available.
- Up to date backup copy of GrSrLic.dat file is available.

Grayteq DLP Clients identify Grayteq DLP Security Server based on its IP address and FQDN name; therefore it is important to install the new running environment on the same IP address and FQDN name. If it is not possible, and the IP address and the FQDN name of Grayteq DLP Security Server had been changed, the following steps has to be done:

- Install Grayteq DLP Security Server in the new environment. It is very important to have the same installation folder as by the previous (e.g. “old”) system.
- Copy GrSrCfg.dat and GrSrLic.dat files into the %ProgramFiles%\Grayteq\DLP\Server\ folder (or into the folder wherever the software were installed) after finishing the installation.

Setting Clients

- Start in “Safe Mode” each and every computer run Grayteq DLP Clients one-by-one. Start a command prompt and navigate to the folder contains Grayteq DLP Client (%ProgramFiles%\Grayteq\DLP\Client).
- Set the following command:
`grclsvc.exe setserver (IP address or FQDN name of the new server).`
This will set by each and every Grayteq DLP Client, to which Security Server will be sent the log files to by the particular Client.

After this, the system will operate based on the last backup configuration.

Loss of function

A loss of function is, if one or more functions of Grayteq DLP malfunction. In this case, the functions and the operation of some Grayteq DLP components have to be checked.

Control of Logging

In case of no log files arrive from some Clients, the operation of such ones has to be checked.

Client status:

Entering into the Security Orchestrator, on the Computer Panel double click on the computer, wherefrom no logs are coming. The status of the Settings: Client has to be “On” status.

Network check:

Check if the network operates properly, computers of Clients and the Security Server are able to communicate with each other.

Client check:

Check whether grclsvc.exe process runs on the given computer. If it does not, start Grayteq Client Service and with the help of the status logs analyze why the service stopped.

Log Filters check:

Check the settings of Log Filters if there are not any falsely set, which filter logs might arrive from the particular Client.

Error handlings, reporting

If a problem comes up during the operation of Grayteq DLP that is not mentioned herein, please indicate it on the following e-mail address: support@grayteq.com

Glossary

A

Name	Description
About	You can find End User License Agreement, support related internet sites, and trademarks in the About area of the Security Orchestrator.
Client	It is the part of Grayteq DLP, which enforces Policies and creates logs on Hosts that it had been installed on. While operating, it transmits events to Security Server, or if the Security Server is inaccessible, stores information locally. The Client deeply infiltrates the Operating System core, so it can provide maximum control over the initiated actions.
Alert	Using Grayteq DLP Security Orchestrator, you can preset special conditions, which trigger In this case, selected Operators receive an e-mail notification.
Archive	Grayteq DLP stores incoming log data in its own, specially designed database. When archiving, a previously active database is to be qualified as archive. When archiving, by using preset conditions, Grayteq DLP closes the database that stores active log data, then opens a new database to ease the load.
Assign	In assignment, you link a created Policy or Policy Group to a specific Host, Host Group or Every Host. So Assign is the operation of applying a Policy at a Host, by dragging a Policy over the name of the desired Host, Host Group holding the Host or Policy Group in Grayteq DLP Security Orchestrator.
Auto Report	With this feature, you can automatically create a File Lifecycle Tracking or a report. This streamlines day-by-day administration. The reports or File Lifecycle Trackings can be created repeatedly in specified intervals, and every time an e-mail notification can be sent to certain operators.

C

Name	Description
Cascade Spool	The Security Server uses an own storage system for the Update packages, Auto Reports and Alerts to store. The size of this can be maximized (Server property panel), and by reaching its size the oldest element is going to be deleted. These types of storages are called Cascade Spool.
Clean up	Process whenever all earlier created Log entries will be deleted from the certain Log entry category.
Client CAL	It is an Client that only starts logging after the user logs in on the Host. In case the user has not logged in on the Host yet, the Grayteq DLP Client does not log events. The previously specified Policies, for example Quarantines are still applied.
Consistency Check	The Security Server is able to check its log files, if those are in intact state. It is able to repair partially or fully the corrupted elements (e.g.: file corruption caused by power-cut). This

Name	Description
	process is called Consistency Check.
Security Orchestrator	It is the part of Grayteq DLP, which can be used to manage the Grayteq Security Server and Hosts. The graphical interface of the Security Orchestrator provides an opportunity to create Policies, assign Hosts to them, query different events, set alert conditions, control Security Server and Client operations, or create File Lifecycle Trackings. The applications also let you download updates, language modules and licenses, activate and assign licenses, install Clients to selected Hosts or update previously installed Clients.

D

Name	Description
DbgHelp component	Redistributable Windows component, with its API reference such information can be retrieved, in case of an application error, by where a developer environment would be required.
Default Operator	After the first installation of the Grayteq DLP Security Server there is only one defined operator in the system, whose only competencies are to create other operators. Default operator user name is John , its password is Doe . You should modify the login parameters of the default operator after the first login. You can change its password, or delete operator John.
Device	Storage or communication capable peripherals in the operating system, which one do not display as a drive. These are hard or impossible to describe for Grayteq DLP with the use of Event Controls, Log Filters, Quarantines or other Policies. These peripherals can have general blocking, allowing or read-only Policies applied to them. Such devices are USB drives, Floppy drives, Infrared or Bluetooth devices, and peripherals attaching to COM and LPT ports.
Dock	Dock is a process when you are placing in the Grayteq DLP Security Orchestrator the used movable panels to any of the sides of the application, filling its whole width or length.
DRP	Disaster Recovery Plan

E

Name	Description
Event	Each action that users perform on files generates event and log entries. Grayteq DLP can differentiate between Create, Read, Modify, Copy, Move, Delete, Run and Stop, Copy, Past, Print, Alert and different System events. Events describe what happened in the system.
Event Control	Use a Filter to specify access policies for files and/or paths. With a Filter, you can set who, when and by what Processes can access or perform specific operations on a File or Path. Filter Policies can apply for negated paths and processes also.
Every Host	It is a special group; to which all Hosts handled by Grayteq DLP and running an Client belong. If a Policy or a Policy Group is assigned to the Every Host group, the assigned Policies apply to all Hosts. When installing a new Grayteq DLP Clients, these

Name	Description
	Policies instantly apply to the new Host.
Existence History	If the appropriate history data is accessible, Grayteq DLP can create a complete existence history for the path. Use this feature to determine when and under what name a file existed on the specified path, and gather information on who and when created and/or deleted it.
Export	You can export predefined Policies and created Reports to external files.

F

Name	Description
Favorites	Definition for items, which ones will be separated and emphasized, in the Grayteq DLP Security Orchestrator's Logs view, for the easier use later.
File Activity	If the appropriate history data is available Grayteq DLP can display events occurred between the attachment and detachment, and related to a specific storage. You can view connections between displayed events, and determine where a file on the storage was placed, or where it came from. If a file was copied from the storage to the Host, you will be able to determine its location.
File Lifecycle Tracking	Use File Lifecycle Tracking (FLT) to track events that occurred to a specific file. You can see where the file came from, who, when and using which processes has used the file, and what iterations exist on various Hosts and/or in storages.
File Lifecycle Tracking from Creation	If the appropriate history data is accessible, Grayteq DLP can create a complete life history for the file. Use File Lifecycle Tracking from Creation to view whether a file under the specified name was created, and view events related to the item. Use this method to determine whether a file under the specified name was created, and who, when and by which processes initiated events on certain hosts and/or storages.
FLT	File Lifecycle Tracking
FQDN	Fully Qualified Domain Name

G

Name	Description
Glue	Glue is a process when the movable panels used in Grayteq DLP Security Orchestrator will be attached to any sides of the application, filling up its whole width or length.

H

Name	Description
Host	In the Grayteq DLP terminology the term Host stands for all units that has a Grayteq Client installed and so is recognized and/or managed by Grayteq DLP. Hosts can be organized into

Name	Description
	groups. The special group Every Host stands for all hosts which have an Client running on it.
Host Group	It is the name of a logic unit, which can contain multiple Hosts or other Host Groups. Host Groups - just like Hosts - can have Policies, Event Controls, Quarantines and other Policies assigned to. Policies assigned to a Host Group will be valid on each Host that is in the Host group.

I

Name	Description
Import	You can load previously defined Policies from external files through the Grayteq DLP interface. During import you might encounter Policies that have the same names as existing Policies. In this case, concatenating a number to it modifies the name of the imported Policy.
Install	You can remotely install Grayteq Clients to Hosts found by Grayteq DLP or gathered from Active Directory in Install menu, by Maintenance view.
Intrusion Prevention	(as a Policy) In the system Zones can be created, which ones can be freely assigned to Hosts, helps to form the security infrastructure of the company.
Inverting	It is a logic operation, when the negative of a stated condition is realized. Grayteq DLP provides an opportunity to apply an easier definable Policy when creating Policies. Typically, when you have to specify many paths for a block, it might be easier to state which paths the condition is not applicable for.

L

Name	Description
License	In the Security Orchestrator, by the Maintenance view, by the License menu you can activate the purchased License, and assign the activated Licenses to Hosts. An Grayteq DLP Client running without a License will not apply any Policies, and the Log Entries created from Events by this Client cannot be viewed.
License Manager	Component of Grayteq where the Licenses want to be used in the system can be handled.
Local item	The certain group of items in Grayteq DLP, which ones are accessible from the logged accounts running the Host with Grayteq DLP Security Orchestrator, and these are stored on the computer of the Operator.
Log Filter	With the Log Filter, it is possible to bypass Log Entries that are not related to user operations, and do not provide substantive information. Examples are temporary files of word processor applications. It is unnecessary to continuously log these into the database. By filtering the Log Entries network traffic and database size can be reduced, and you will be able to shorten time needed to identify incidents, and improve Security Server performance.

Name	Description
Log item category	Collective description of all types of logs. Such categories are the Monitor, Report, FLT, etc.

M

Name	Description
Maintenance	In the Grayteq DLP terminology the Maintenance means in the Security Orchestrator, the Maintenance view. With its help you can install Clients on Hosts, download and install Upgrades, furthermore activate and assign Licenses to Hosts. In this view the Operators, Archives, Servers, Server Log and Server settings are available also.
Module	Grayteq DLP consists of multiple modules, each responsible for different tasks. Security Server stores the Policies, transmits those for Clients, and stores incoming Log Entries. The Security Orchestrator is the graphical interface, through which the network can be managed, the devices can be queried and command can be submitted to the Clients. Clients which run on Hosts and apply commands submitted, enforces Policies, and sends Log Entries on events to the Security Server.
Monitor	The page provides a continuous, real-time display of events related to the Grayteq DLP Clients. Clients are constantly sending events that are listed on the Monitor page.

N

Name	Description
Negate	Inverting is a logical operation that describes a conditions reverse value. The Grayteq DLP system enables you having a Policy, which only allows Printers, Paths, and Applications, which are NOT listed in the Policies.
Normal	Process/function, whenever the earlier selected Log entry gets back to the Grayteq DLP Security Orchestrator. This function is automatic by the closing of selected Log entries.

O

Name	Description
Operator	Grayteq DLP provides an opportunity to define multiple Operators, who can have separate permissions. According to this, Operators can perform different actions, so tasks and responsibility can be divided. For example, define an Operator who can create Policies, but will not be able to create Reports, or an Operator who is only allowed to set other Operators' permissions.

P

Name	Description
------	-------------

Name	Description
Panels	Stands for all interfaces that can be used for managing and maintaining the system and for setting Policies.
Printer	In Grayteq DLP terminology a Printer is a Printer Policy, which can be used to enable or disable the use of specific printers. The created Policy can contain one Printer or a group of Printers. By assigning it to a Host you can specify if it is possible to print from the specific Host or not.
Printer List	A special group, in which all printers identified by Grayteq DLP are automatically listed. The list of the printers in this group is freely expandable. When creating Printer Policies, you can select Printers to be controlled from this list.

Q

Name	Description
Quarantine	It is a document space which can be used to guarantee that any operation can be performed on protected files within the document space, but no data is exiting this space unless this is specifically granted. Quarantines can be useful, when you have to provide access to sensitive documents for a user, but you do not want to enable the user to transfer the information elsewhere.

R

Name	Description
Recent Items	List of the last items edited or opened with the Wizard.
Remote Items	Totality of items found in Grayteq DLP system, which ones can be found on the Grayteq DLP Security Server and can be used and assigned actively.
Remote template	Totality of items found in Grayteq DLP system, which ones can be found on the Grayteq DLP Security Server and other items can be created from them. The items in this category cannot be run and cannot be assigned to Hosts, Host Groups or users.
Report	Use Reports to create queries. You can query any events occurred in a Security Server, and specify whether to inspect one or more specific Hosts, Events, Paths, Users, or a specific time interval for events.
Result	Result of events. If you set a Policy that denies access to a specific file, and a user initiates an operation which is in conflict with this Policy, the result of the event is "Blocked". If the event is not in conflict with any Policy, the result is "OK".
Policy Group	It is a container for holding Policies. A Policy Group can contain Printer, Event Control, Log Filter, and Quarantine Policies, or another Policy Group. If there are more Hosts or Host Groups that the same Policies apply to, you have the option to create Policy Groups to simplify network maintenance.

S

Name	Description
Seek Origin	If the appropriate history data is accessible, Grayteq DLP can create a complete life history for the file. Use the Seek Origin method to determine when and by whom the specified file was created, in other words, where it came from. Seek Origin resolves all events through multiple files, multiple rename, move or copy operations, until the first creation time is uncovered. This way you can discover not only events related to the file created under the certain name, but look for the original document irrespectively for the original file name or location.
Seek Origin and Generate FLT	If the appropriate history data is accessible, Grayteq DLP can create a complete life history for the file. The Seek Origin and Generate FLT method can help determine when a file was created and who that file was created by, in other words, what the origin of the file is, and resolve all events from that point. Seek Origin resolves all events through multiple files, multiple rename, move or copy iterations, until the first creation time is uncovered. This way you can discover not only events related to the file created under the certain name, but look for the original document irrespectively for the original file name or location. Using the discovered origin, you have the option to display events related to the file, determine who, when and by which processes executed operations on the original file, and what type of modifications of the original file exist throughout hosts and/or storages.
Security Server	It is the central module of Grayteq DLP. Its task is to store policies and transmit them to the Clients, and to receive, to process and to transmit incoming log data to the Security Orchestrator when creating a report. The Security Server component monitors incoming log data, and can generate alerts depending on previously set alert conditions. You can also fully manage the network through the Security Server: handle licenses, activation, updates and installations.
Server CAL	A Client that starts logging at the operating system startup. Grayteq DLP Client creates and forwards log entries even when no one is logged in to the Security Server.
SLT	Storage Lifecycle Tracking
Snapshot	About the activity of the given user, at the time of the log entry, a screenshot made by the Client.
Standard File Lifecycle Tracking	If the appropriate history data is accessible, Grayteq DLP can create a complete life history for the file. Use the Standard File Lifecycle Tracking to track events related to a file from a specified time. You can see where the file came from, who, when and using which processes has used the file, and what iterations exist on various hosts and/or in storages in the specified interval.
Storage	Grayteq DLP can handle any attached device that is represented as a file system for the operating system. This allows the assignment of access policies to new and unknown storage devices, irrespectively their manufacturer and connection interface (USB, PCMCIA, Bluetooth, etc.). At the moment of attaching, the Client activates the Policy applied to them, and creates a log on

Name	Description
	occurring events. ■ (as a Policy) Policies can be created for the storages, which can be assigned to the Computers or Users, after it comes into operation and allows or blocks the certain Storage.
Storage Activity	If the appropriate history data are accessible, Grayteq DLP can create a complete usage life history for different Storages. Use this feature to determine which Hosts and when was a specific Storage attached to or detached from.
Storage Lifecycle Tracking	Use Storage Lifecycle Tracking (SLT) to determine when and which Host was a specific Storage attached to or detached from, and that who, when and by which processes performed operations on it.
StringIndex	Security Server does not store redundant the text based information in the interest of the optimal event log size. The same text information will not be stored in multiple ways; it gets into a reference control service only. This text reference control service is called StringIndex service.
Support ID	Errors can occur during the operation of the Security Server, which ones are depending of the parameters of the environment. The purpose of the Support ID is to detect these types of errors, and to solve it without the help of the Support Team.

T

Name	Description
TimeIndex	Security Server handles the log files in a time order. To be able to handle this, there is a need of extra information besides the log events. This is called TimeIndex files.
TimeIndex Recreation	The self-correcting process of the corrupted TimeIndex files, which process is done automatically, if the Security Server recognizes error in the TimeIndex files, or this can be turned on from the Server settings panel. In this case the Security Server, by its next restart will check the TimeIndex files definitely. The process can take longer by larger log file size.

U

Name	Description
Update	You can download Upgrades from the Grayteq DLP homepage, or load already downloaded Upgrades into the Security Server what you can find in the Security Orchestrator, by the Maintenance view, by the Update menu.
Upgrade	You can install downloaded Upgrades to selected Hosts or Host Groups, by the Maintenance view, by Upgrade menu. Here you can also view which version of the Grayteq DLP Client is installed on specific Hosts, and find information regarding to the Version History of certain Hosts also.
Users	In the Grayteq terminology, every unit is called a User, which one is representing one user in the company's infrastructure and which a Policy can be assigned to. In this case the assigned Policy will be active by all Clients and will be executed on the certain User.

V

Name	Description
Views	Such surface areas managing the system in Grayteq DLP Security Orchestrator, which ones are typically for displaying and requesting information, furthermore for handling Policies; or with its help the installation, update and licensing of Clients, and the fine-tuning of the system can be done.

W

Name	Description
Wizard	Such surface areas, with its use the system settings can be performed.